vCenter Configuration Manager Installation and Getting Started Guide

vCenter Configuration Manager 5.3

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000456-00

vmware

You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2006-2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Copyright 2

About This Book 9

Preparing for Installation 11
- **Using Installation Manager** 12
- **Understanding Installation Configurations** 12
- **Understanding Tools Installation** 13
- **Checking Prerequisites for Installation** 13
  - **Hardware and Software Requirements** 13
  - **Administration Rights** 13
  - **Default Network Authority Account** 13
  - **Default Collector Services Account** 14
  - **VMware Application Services Account** 14
  - **VCM Remote Virtual Directory** 14
  - **Secure Communications Certificates** 15
  - **Server Authentication** 15
- **Understanding VCM's Use of FIPS Cryptography** 17
  - **VCM's Use of Microsoft Cryptographic Service Providers (CSPs) for Windows Machines** 17
  - **Cryptography for UNIX/Linux Platforms** 17
  - **Cryptography used in VCM Software Components** 18
  - **Supported Windows and UNIX Platforms** 18

Installing VCM Using Installation Manager 19
- **Using the Installation Manager** 19
  - **Navigating VCM Installation Manager Screens** 19
  - **Installing VCM and the Related Components** 19

Upgrading VCM and Related Components 35
- **Prerequisites** 35
  - **Backup and Recovery** 35
  - **Assumptions for Upgrading Your VCM Collector and Database** 36
- **Upgrading to VCM 5.3** 36
  - **Upgrading the VCM Database Only** 36
  - **Upgrading VCM on a 32-Bit System** 36
  - **Upgrading to a 64-Bit System** 36
  - **Before Upgrading** 37
  - **Performing the Upgrade** 37
- **Upgrading Existing Windows Agents** 38
- **Upgrading Existing Remote Clients** 39
- **Upgrading Existing UNIX Agents** 40
  - **To Upgrade the UNIX Agent(s) with a Local Package** 40
  - **To Upgrade the UNIX Agent(s) with a Remote Package** 41
- **Upgrading VCM for Virtualization** 42
  - **Upgrading an Agent Proxy Machine** 43
  - **Upgrading the vSphere Client VCM Plug-in** 45

Getting Started with VCM Components and Tools 47
- **Understanding User Access** 47

Launching and Logging Onto VCM 48
How to Launch VCM and Log On 48
Getting Familiar with the Portal 48
General Information Bar 49
Portal Toolbar 49
Sliders 50
Where to Go Next 52

Getting Started with VCM 53
Discover, License, and Install Windows Machines 53
Verifying Available Domains 53
Checking the Network Authority 54
Assigning Network Authority Accounts 55
Discovering Windows Machines 56
Licensing Windows Machines 59
Installing the VCM Windows Agent on your Windows Machines 61
Performing an Initial Collection 67
Exploring Windows Collection Results 68
Getting Started Collecting Windows Custom Information 72
Discover, License, and Install UNIX/Linux Machines 80
Adding UNIX/Linux Machines 81
Licensing UNIX/Linux Machines 82
Installing the Agent on UNIX/Linux Machines 83
Performing a UNIX/Linux Collection 90
Exploring UNIX/Linux Collection Results 91
Discover, License, and Install Mac OS X Machines 94
Getting Started with VCM for Mac OS X 94
Adding Mac OS X Machines 94
Licensing Mac OS X Machines 96
Installing the Agent on Mac OS X Machines 97
Performing a Mac OS X Collection 103
Exploring Mac OS X Collection Results 106
Discover, License, and Collect Oracle Data from UNIX Machines 108
Adding UNIX Machines Hosting Oracle and Installing the Agent 109
Discovering Oracle Instances 109
Creating the Oracle Collection User Account 110
Performing an Oracle Collection 114
Exploring Oracle Collection Results 114
Reference Information about Oracle 114
Customize VCM for your Environment 115
How to Set Up and Use VCM Auditing 116

Getting Started with VCM for Virtualization 117
Virtual Environment Configuration 117
ESX 2.5/3.x,vSphere 4, and ESXi Servers Collections 118
vCenter Server Collections 118
Configuring Agent Proxy Virtualization Collections 118
Configuring Agent Proxy Machines 120
Licensing Agent Proxy Machines 120
Installing the Agent on the Agent Proxy Machine 121
Performing a Collection Using the Machines Data Type 121
Installing Agent Proxies 122
Configuring ESX/vSphere Servers 123
Copying Files to the ESX/vSphere Server 124
Running Scripts on the ESX/vSphere Server 124
Adding ESX/vSphere Servers to VCM 125
Licensing the ESX/vSphere Server in VCM 126

Licensing ESX/vSphere Server Machines as Virtual Machine (VM) Hosts 127
Configuring Web Services for ESX/vSphere Server Communication 128
Adding the Web Services User to the Administrator Role Using the VI Client/vCenter Client 129
Installing the ESX Web Services Certificate on the Agent Proxy Machine 130
For ESX 2.5.x Only: Setting Up VirtualCenter to Collect Virtualization Data 134
Adding Web Services Settings 134
Performing an Initial Virtualization Collection 134
Exploring Virtualization Collection Results 135
Configuring vCenter Server Data Collections 137
vCenter Server Collection Prerequisites 137
Collecting vCenter Server Data 141
Reviewing Collected vCenter Server Data 142
Troubleshooting vCenter Server Data Collections 142
About the vSphere Client VCM Plug-in 143
Registering the vSphere Client VCM Plug-in 143
Configuring the vSphere Client VCM Plug-in Integration Settings 144
Getting Started with the vSphere Client VCM Plug-in 145
Upgrading the vSphere Client VCM Plug-in 146
Further Reading 146

Getting Started with VCM Remote 147
Getting Started with VCM Remote 147
Installing the VCM Remote Client 148
Installing the Remote Client manually 149
Making VCM Aware of VCM Remote Clients 156
Configuring VCM Remote Settings 156
Creating Custom Collection Filter Sets 156
Specifying Custom Filter Sets in the VCM Remote Settings 156
Performing a Collection Using VCM Remote 157
Exploring VCM Remote Collection Results 157

Getting Started with VCM Patching 159
Getting Started with VCM Patching 159
Getting Started with VCM Patching for Windows Machines 159
Check for Updates to Bulletins 159
Collect Data from Windows Machines Using the VCM Patching Filter Sets 160
Launch an Assessment 161
Explore VCM Patching Windows Assessment Results 165
Deploy Patches to Windows Machines 165
Getting Started with VCM Patching for UNIX/Linux Machines 168
Getting Started 168
Check for Updates to Bulletins 169
Collect Assessment Data from UNIX/Linux Machines 169
Explore Assessment Results and Acquire the Patches 173
Deploy Patches to UNIX/Linux Machines 175
How the Deploy Action Works 176
Further Reading 177

Getting Started with Software Provisioning 179
VMware vCenter Configuration Manager Package Studio 179
Software Repository for Windows 179
Package Manager for Windows 179
Overview of Component Relationships 180
Installing the Software Provisioning Components 180
Install Software Repository for Windows 181
Software Repository Structure 182

Manually Uninstall the Repository 182
Install Package Studio 182
Manually Uninstall Package Studio 184
Install Package Manager on Managed Machines 184
Using Package Studio to Create Software Packages and Publish to Repositories 185
Creating Packages 185
Using VCM Software Provisioning for Windows 186
Prerequisites 186
Collect Package Manager Information from Machines 187
Collect Software Repository Data 187
Add Repository Sources to Package Managers 188
Install Packages 189
Related Software Provisioning Actions 190
Viewing Provisioning Jobs in the Job Manager 190
Creating Compliance Rules based on Provisioning Data 190
Creating Compliance Rules containing Provisioning Remediation Actions 191
Further Reading 193

Getting Started with VCM Management Extensions for Assets 195
Getting Started with VCM Management Extensions for Assets 195
Review Hardware and Software Configuration Item Fields 195
Modifying Hardware Configuration Item Fields 196
Modifying Software Configuration Item Fields 198
Adding Hardware Configuration Items 200
Editing Values for Devices 200
Modifying Other Devices 201
Adding Software Configuration Items 202
Further Reading 203

Getting Started with VCM Service Desk Integration 205
Getting Started with Service Desk Integration 205
Service Desk Integration in the Console 205
Service Desk Integration in Job Manager 206
Further Reading 207

Getting Started with VCM for Active Directory 209
Making VCM Aware of Domain Controllers 209
Confirming the Presence of Domains 210
Adding and Assigning Network Authority Accounts 211
Discovering Domain Controllers 211
Verifying Domain Controller Machines in Available Machines 213
Licensing and Deploying the VCM Agent 213
Performing a Machine Data Type Collection 216
Configuring VCM for Active Directory as an Additional Product 216
Deploying VCM for AD to the Domain Controllers 216
Running the Determine Forest Action 218
Running the Setup DCs Action 218
Performing an Active Directory Data Collection 220
Exploring Active Directory Collection Results 223
Further Reading 226

Getting Started with VCM for SMS 227
Getting Started with VCM for SMS 227
Making VCM Aware of the SMS Servers 227
Performing SMS Server Collections 228
Performing SMS Client Collections 229
Exploring SMS Collection Results 229

Viewing SMS Dashboards 229
Viewing SMS Server Data 230
Viewing SMS Client Data 231
Viewing SMS Reports 232
Further Reading 233

Getting Started with Windows Server Update Services 235
Getting Started with Windows Server Update Services 235
Making VCM Aware of the WSUS Server 235
Performing WSUS Server Collections 236
Performing WSUS Client Collections 236
Exploring WSUS Collection Results 237
Viewing WSUS Clients 237
Viewing WSUS Reports 238
Further Reading 238

Accessing Additional Compliance Content 239
Locating the Content Directory 239
Launching the Content Wizard to Import Relevant Content 239
Exploring Imported Content Results in the Portal 239

Installing and Getting Started with VCM Tools 241
Installing the VCM Tools Only 241
Foundation Checker 242
VCM Job Manager Tool 242
VCM Import/Export and Content Wizard (CW) 243
VCM Import/Export 244
Content Wizard 245

Maintaining VCM After Installation 247
Customize VCM and Component-specific Settings 247
Configure Database File Growth 249
Configure Database Recovery Settings 250
Create a Maintenance Plan for SQL Server 2005 250
Incorporate the VCM CMDB into your Backup/Disaster Recovery Plans 258

Troubleshooting Problems with VCM 259
Evaluating Missing UNIX Patch Assessment Results 259
Resolving Reports and Node Summaries Problems 260
To Resolve the Problem 260
Resolving Protected Storage Errors 260
To Resolve the Problem 261
Resetting the Required Secure Channel (SSL) 261
Updating the Web.config Configuration File 261
Updating the VCM Virtual Directory 262
Updating the IIS Settings in VCM 262
Resolving a Report Parameter Error 262

Configuring a Collector as an Agent Proxy 265
Verifying Membership to CSI_COMM_PROXY_SVC on the Agent Proxy Machine 265
Generating Key Pairs on the Agent Proxy Machine 266
Uploading Keys to the Database 266

Index 267

About This Book

This guide, *VCM Installation and Getting Started Guide*, describes the steps you must take in order to ensure a successful VMware vCenter Configuration Manager (VCM) installation. This document contains the following information:

- Preparing for the VCM installation.
- Installing VCM.
- Getting started with VCM and its components.
- Maintenance and troubleshooting.

Read this document and complete the associated procedures to prepare for a successful installation.

The *VCM Installation and Getting Started Guide* covers VCM, Foundation Checker, and Service Desk Connector.

Intended Audience

The information presented in this manual is written for system administrators who are experienced Windows or UNIX/Linux system administrators and who are familiar with managing network users and resources, and performing system maintenance.

To use the information in this guide effectively, you must have a basic understanding of how to configure network resources, install software, and administer operating systems. You also need to fully understand your network's topology and resource naming conventions.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the *VCM Hardware and Software Requirements Guide*, *VCM Foundation Checker User's Guide*, VCM online Help, this manual, and other associated documentation.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support	To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support. Customers with appropriate support contracts should use telephone support for priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.
Support Offerings	To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.
VMware Professional Services	VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Preparing for Installation

1

This chapter provides important information that will help you prepare to install VCM components and tools in your enterprise. This chapter contains the following sections:

- Using Installation Manager: Provides an overview of Installation Manager, which is used to install and activate all VCM components and tools.
- Understanding Installation Configurations: Describes the supported installation configurations for VCM.
- Understanding Tools Installation: Explains how VCM tools are installed.
- Checking Prerequisites for Installation: Lists the prerequisites you should complete prior to using VCM Installation Manager to perform the installation.

For an overview of the security precautions you should take before installing VCM, see the VCM Security Environment Requirements Technical White Paper on the VMware vCenter download site.

This document assumes that your hardware and software configuration meets the requirements described in *VCM Hardware and Software Requirements Guide*. If you have not already done so, verify that your configuration meets the installation requirements by performing a Tools Only installation of VCM Foundation Checker, and then running it once it is installed. If VCM Foundation Checker does not return any errors, then you are ready to proceed. For more information on performing a Tools only installation, see "Installing and Getting Started with VCM Tools" on page 241. If you choose to install and run the Foundation Checker before installation, it is important to uninstall the Foundation Checker before running the Installation Manager.

Using Installation Manager

Installation Manager performs new installations as well as upgrades, and provides a highly simplified process for installing components and tools. Installation Manager has a straightforward interface that steps you through the entire installation or upgrade process.

Installation Manager:

- Performs the checks to ensure the machine(s) meets the hardware and software prerequisites necessary for installing.
- Provides confirmation of the license file you are applying during installation.
- Installs VCM and all of its components and tools in the appropriate order on your machine(s).
- Tests each progressive step during the installation to ensure that all components were successfully installed and that the licensed components were successfully activated.

In addition, Installation Manager operates with minimal user input, and provides clear feedback on progress throughout the entire installation process.

Installation Manager installs VCM and all of its components on your machine, even those that you have not purchased. However, only the components that have been purchased are licensed by your license file. This enables you to purchase more licenses later, and thereby activate additional components that are already installed.

To install VCM and all of its components and tools for the first time, follow the procedures described in Using Installation Manager.

IMPORTANT When upgrading to VCM 5.3.0, be aware that you can use Installation Manager to upgrade from VCM 4.11.1 or later.

When performing a new installation or an upgrade, you must have the previous license file available and specify the path to the license file during the installation. Installation Manager will use the license file to activate the components that you have purchased. If you do not have the license file from VCM 4.11.1 or later, contact VMware Customer Support.

Understanding Installation Configurations

Before proceeding, you must have already configured your hardware and installed all of the prerequisite software based on the information in the *VCM Hardware and Software Requirements Guide*. VCM has two supported installation configurations: the default, single machine installation in which all components and tools are installed on a single machine; and the advanced, "split" installation in which the Collector and the database are installed on two separate machines.

IMPORTANT A split installation across two machines should be used only when your corporate policy requires you to have your SQL Server data stored on a centralized database server. Split installations are implemented and supported only by VMware Customer Support. Installation instructions are not provided in this manual.

Refer to the *VCM Hardware and Software Requirements Guide* for a detailed diagram of a complete installation.

Understanding Tools Installation

The VCM tools include:

- Foundation Checker
- Job Manager
- Import/Export and Configuration Content Wizard (CCW)
- Web Services Toolkit

All of the tools are automatically installed. Installation procedures are provided in "Using Installation Manager" on page 12.

VCM tools may be installed separately on a non-Collector machine as appropriate. To install Tools Only, follow the installation procedures in "Installing and Getting Started with VCM Tools" on page 241

Checking Prerequisites for Installation

This section lists the prerequisites that you should complete prior to using Installation Manager.

Hardware and Software Requirements

Your hardware and software configuration must meet the requirements described in the *VCM Hardware and Software Requirements Guide* before you can proceed with your installation.

IMPORTANT You can ensure a smooth and efficient installation by validating that your machines meet all the requirements by performing a Tools Only installation of Foundation Checker (see "Installing and Getting Started with VCM Tools" on page 241) and running it once it is installed. If Foundation Checker returns no errors, then you are ready to proceed. If your machine(s) do not meet these requirements, the installation cannot proceed.

If you are installing on HP-UX 11.11, Patch PHSS_30966 is required for the HP-UX Agent. If you need assistance, contact VMware Customer Support.

Administration Rights

The User Account of the person performing your installation or upgrade must be all of the following:

- A system administrator on the machine(s) on which the installation or upgrade is being performed, **and**
- A system administrator on the database instance that will be used, **and**
- A member of a domain.

The installing User Account should **not** be the account used to run the SQL Server Services; nor, after installation, should you create a VCM user with the SQL Server Services account credentials.

Default Network Authority Account

The default network authority account must be specified during the installation process. This account, which often is the system administrator's (for example, a Domain Admin in the Local Admin Group), must be set up in the Local Administrators group on each machine prior to installation. This should have already been completed following the checklist in the *VCM Hardware and Software Requirements Guide*.

The Local System account named NT AUTHORITY\System has unrestricted access to all local system resources. This account is a member of the Windows Administrators group on the local machine, and a member of the SQL Server sysadmin fixed server role. If the NT AUTHORITY\System account does not have access to the VCM installation binary files (possibly because someone removed the account or inherently removed access), the installation will result in an "access denied" error in the first step. Details of this error are not stored in the VCM error log. The solution is to grant access to the NT AUTHORITY\System account from the installation source directory (right-click the folder, select the Security tab, and then make sure the user or user's group has Full Control of the file/folder). Then run the installation again.

NOTE The network authority account can be changed later in VCM at **Administration | Settings | Network Authority**.

Default Collector Services Account

The default services authority account must be specified during the installation process. This account, which may not necessarily be the system administrator's, must exist in the Local Administrators group on the Collector machine. In addition, this account must not be a LocalSystem account.

IMPORTANT If the password for your services account changes, you must also change the password in both the Services Management and Component Services DCOM Config consoles.

To change your services password in the Services Management console, click **Administrative Tools | Services**. Locate all of the services that use the services account to log on. Right click each of these services, then select **Properties**. Click the **Log On** tab, and then update the password field to reflect your new password.

To change your services password in the Component Services DCOM Config console, click **Administrative Tools | Component Services**. Expand the Component Services node, then select **Computers | My Computer | DCOM Config**. Right click the **LicenseDcom** file, then select **Properties**. Click the Identity tab, and then update the password field to reflect your new password.

VMware Application Services Account

The VMware Application Services Account must be a domain user. Because this account will have full administrative authority for the CSI_Domain database, it should never be used as a VCM login or for any other purpose.

VCM Remote Virtual Directory

The VCM Remote Virtual Directory account must be specified during the installation process. This account should not be the same account you used for your Default Network Authority Account and/or your Default Services Account to reduce the chances of a security risk to those accounts.

NOTE The service account can be changed later if necessary using the IIS Management console.

Secure Communications Certificates

VCM uses Transport Layer Security (TLS) to secure all HTTP communication with Windows and UNIX Agents in HTTP mode (includes all UNIX Agents and Windows Agents in HTTP mode). TLS uses certificates to authenticate the Collector and Agents to each other. You must specify certificates for the Collector and for the Enterprise during the installation process. If you plan to use your own certificates, familiarize yourself with the certificate names so that you can select them during installation.

To be valid, a Collector certificate must meet the following criteria:

- The Collector certificate must be located in the local machine personal certificate store.
- The Collector certificate must be valid for Server Authentication. If any Enhanced Key Usage extension or property is present, it must include the Server Authentication OID 1.3.6.1.5.5.7.3.1. If the Key Usage extension is present, it must include DIGITAL_SIGNATURE.
- The Collector certificate must not be expired.

If you want Installation Manager to generate the Collector and Enterprise certificates for you, select the Generate option during installation.

NOTE If you will be installing more than one Collector that will communicate with the same Agent(s), or you plan to replace/renew your certificates at a later date, there are special considerations for generating and selecting certificates in VCM Installation Manager. For more information about VCM and Transport Layer Security (TLS), see Transport Layer Security Implementation for VCM.

Server Authentication

Server Authentication is a method of authenticating the server to the client. VCM supports server authentication. In VCM environments where TLS is employed, VCM Agents verify the identity of the Collector (or Collectors) through the use and verification of certificates (over HTTP).

Typically, the server authenticates a client/user by requiring information, such as a user name and password. When server authentication is used, the client/user verifies that the server is valid. To accomplish this verification using TLS, the server provides a certificate issued by a trusted authority, such as Verisign®. If your client web browser has the Verisign® Certified Authority certificate in its trusted store, it can trust that the server is actually the web site you are accessing.

TLS uses certificates managed by a public key infrastructure (PKI) to guarantee the identity of servers and clients. A certificate is a package containing a public key and information that identifies the owner and source of that key, and one or more certifications (signatures) verifying that the package is authentic. To sign a certificate, an issuer adds information about itself to the information already in the certificate request. The public key and identifying information are hashed and signed using the private key of the issuer's certificate.

Certificates are defined by the X.509 RFC standard, which includes fields that form a contract between the creator and consumer. The Enhanced Key Usage extension specifies the use for which the certificate is valid, including Server Authentication.

Enterprise and Collector Certificates

An Enterprise Certificate and one or more Collector Certificates enable secure HTTP Collector-Agent communication in VCM. The Enterprise Certificate enables VCM to operate in a multi-Collector environment. Agents have the Enterprise Certificate in their trusted certificate stores, which they use implicitly to validate any certificate issued by the Enterprise Certificate. All Collector Certificates are expected to be issued by the Enterprise Certificate, which is critical in environments where a single Agent

is shared between two collectors.

Server Authentication is required to establish a TLS connection with an Agent. All Collectors should have a common Enterprise Certificate. Each Collector Certificate is issued by the Enterprise Certificate, and is capable of Server Authentication.

- The Collector Certificate is used to initiate and secure a TLS communication channel with an HTTP Agent. The Agent must be able to establish that the Collector Certificate can be trusted, which means that the Collector Certificate is valid and the certification path starting with the Collector Certificate ends with a trusted certificate. By design, the Enterprise Certificate is installed in the Agent's trusted store, and the chain ends with the Enterprise Certificate.
- A Collector Certificate can also be used to issue Agent certificates. As long as all Collector Certificates are issued by the same Enterprise Certificate, any Agent Certificate may be issued by any Collector Certificate, and all Agents will be able to trust all Collectors. Similarly, all collectors will be able to validate all Agent Certificates. Agent Certificates are used for Mutual Authentication only. Mutual authentication is supported, but requires interaction with VMware Customer Support and a Collector Certificate that also has certificate signing capability.
- The Collector Certificate and associated private key must be available to the Collector. This certificate is stored in the (local machine) personal system store.

Collector Certificates in VCM must adhere to the requirements specified above in Secure Communications Certificates.

Delivering Initial Certificates to Agents

VCM Agents use the Enterprise Certificate to validate Collector Certificates. Therefore, the Agent must have access to the Enterprise Certificate as a trusted certificate. In most cases, VCM will deliver and install the Enterprise Certificate as needed.

- Installing the Agent from a Disk (Windows® only): The VCM Installation DVD does not contain customer-specific certificates. If HTTP is specified, the manual VCM Installer requests the location of the Enterprise Certificate file during the installation. You must have this file available at installation time. The certificate file (with a .pem extension) can be copied from the CollectorData folder of the Collector. This will be the case whether you run the manual installer directly (CMAgentInstall.exe) or use the "Agent Only" option from the DVD auto-run program.
- Using CMAgentInstall.exe to Install the Agent (Windows® only): CMAgtInstall.exe or CMAgent[version].msi is the manual Agent installer program. The manual installer will request the location of the Enterprise Certificate file, if HTTP is specified. You must have this file available at installation time. The certificate file can be copied from the CollectorData folder of the Collector.
- MSI Install Package: If HTTP is specified, the MSI agent install package also requires access to the .pem file.
- Installing the Agent for UNIX/Linux: See Installing the VCM Agent on UNIX/Linux Machines in this document.

Installing the Agent Using a Provisioning System

For Windows®, the manual installation program is available in .exe and .msi formats. Both versions allow the Enterprise Certificate file to be specified with a command line switch. The certificate installation step may also be omitted with a command line switch. When these programs are run through a provisioning system, you must ensure that the Enterprise Certificate is available (and still secure), and configure the program options appropriately. Alternatively, you may choose to push the Enterprise Certificate to Agents by some other means and configure the provisioning system to omit certificate installation.

For UNIX/Linux, each UNIX/Linux installation package is targeted for one or more supported platforms. To install the UNIX/Linux Agent using a provisioning system, extract the installation package as appropriate and then deploy the extracted file with the provisioning system. The Enterprise Certificate is embedded in the installation package on the collector.

For more information about Installing the Agent on UNIX/Linux Machines and UNIX/Linux packages and platforms, refer to section Installing the VCM Agent on UNIX/Linux Machines.

Understanding VCM's Use of FIPS Cryptography

Federal Information Processing Standards (FIPS) are developed by the US National Institute of Standards (NIST) and the Canadian Communications Security Establishment (CSE). VCM incorporates cryptography as set forth in the FIPS standards. Components of VCM use cryptography to protect the confidentiality, integrity, availability, and authenticity of customer data. The FIPS standards require adherence by VCM to the following standards:

- FIPS 46-3: Data Encryption Standard (DES)
- FIPS 81: DES Modes of Operation
- FIPS 113: Computer Data Authentication
- FIPS 171: Key Management
- FIPS 180-1: Secure Hash Standard (SHA-1)
- FIPS 186-2: Digital Signature Standard (DSA) and Random Number Generation (RNG)
- FIPS 198: Message Authentication Codes (MACs) using SHA-1
- FIPS 197: Advanced Encryption Standard (AES) Cipher
- FIPS 200: Federal Information Security Management Act (FISMA)
- SP 800-2: Public Key Cryptography (including RSA)
- SP 800-20: Triple DES Encryption (3DES) Cipher

VCM's Use of Microsoft Cryptographic Service Providers (CSPs) for Windows Machines

On Windows machines, VCM uses cryptography by way of the Microsoft CryptoAPI, which is a framework that dispatches to Microsoft Cryptographic Service Providers (CSPs). CSPs are not shipped with VCM or installed by VCM, but instead are part of the security environment included with Microsoft Windows. In the configurations supported by VCM, these CSPs are FIPS 140-2 validated.

Cryptography for UNIX/Linux Platforms

On UNIX/Linux platforms, the VCM Agent uses the cryptography of the OpenSSL v0.9.7 module. This cryptographic library is installed with the VCM Agent.

Cryptography used in VCM Software Components

VCM uses various software components that also use cryptography. Microsoft's IIS, Internet Explorer, and SChannel (SSL/TLS) systems also call the CryptoAPI, and thus use the Windows FIPS-validated modules. VCM for Virtualization uses ActiveX COM components for SSH and SFTP, and for wodSSH, wodSFTP, and wodKeys (by WeOnlyDo! Software at www.weonlydo.com), which utilize the FIPS-certified OpenSSL crypto library. wodSSH is used for windowless communication with remote console-type services in unattended mode on the VCM for Virtualization Agent Proxy's host, which is a Windows platform.

Table 1-1. Installed or Used Crytography Modules

System	Platform	OpenSSLFIPS 1.1.2	OpenSSLFIPS 1.1.1	OpenSSLCrypt 0.9.7	Crypto++	CryptoAPI
UI	Windows					Used
VCMServer	Windows				Installed	Used
Virt Proxy	Windows	Installed				Used
AD Agent	Windows					Used
Win Agent	Windows					Used
UNIX Agent	HP/UX			Installed	Installed	
	AIX			Installed	Installed	
	Solaris			Installed	Installed	
	Debian		Installed		Installed	
	Red Hat		Installed		Installed	
	SUSE		Installed		Installed	
ESX Server	All	No cryptography modules are used or installed on ESX.				

Supported Windows and UNIX Platforms

For a list of supported Windows and UNIX platforms, and their architectures, see the *VCM Hardware and Software Requirements Guide*. For information about TLS, see *Transport Layer Security (TLS) Implementation for VCM* located on the VMware vCenter download site.

Installing VCM Using Installation Manager 2

This chapter explains how to use VCM Installation Manager to install VCM and all of its components and tools. To install only the VCM tools, follow the installation procedures in "Installing and Getting Started with VCM Tools" on page 241.

IMPORTANT When performing an upgrade to VCM 5.3.0, be sure to read Upgrading VCM and Related Components.

This chapter provides a step-by-step guide to the Installation Manager.

CAUTION Before Installing VCM 5.3.0 on a 32-bit System, check for the following registry entry, and rename or remove it if it exists: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node`. VCM 5.3.0 uses this registry entry to detect whether the system is a 32-bit or 64-bit operating system.

Using the Installation Manager

The Installation Manager checks your system to ensure it is properly configured, and then installs the licensed components based on the options selected during the installation process.

Navigating VCM Installation Manager Screens

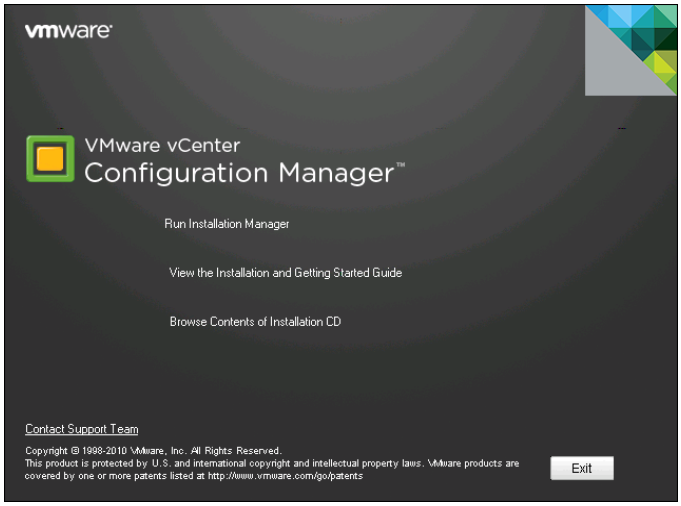
Every VCM Installation Manager screen shows the progress of the installation in the left-most pane. VCM Installation Manager also has the following buttons available at the bottom of every screen:

- **Help:** Opens the *VCM Installation and Getting Started Guide*.
- **Back, Next:** Navigates to the previous or next screen in the installation process, respectively.
- **Cancel:** Exits the installation. If you click **Cancel**, a confirmation pop-up dialog box appears. If you click **OK** in this dialog box, Installation Manager will close. No state information is saved. Any information you have entered thus far during the installation process is lost.

Installing VCM and the Related Components

Follow these steps to start and run the Installation Manager. Be sure to read through the detail about each configurable component as it is presented to make sure you are supplying the appropriate information, as the defaults may not fit your configuration. If you are upgrading VCM or SQL Server, or are upgrading to a 64-bit system, see "Upgrading VCM and Related Components" on page 35.

1. Insert the installation CD into the machine on which you are installing VCM and all of its components. The installation screen appears.

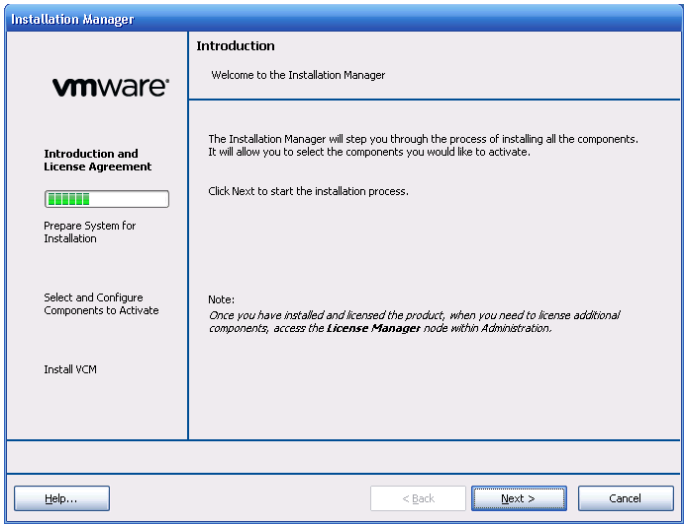

vmware
VMware vCenter
Configuration Manager™
Run Installation Manager
View the Installation and Getting Started Guide
Browse Contents of Installation CD
Contact Support Team
Copyright © 1998-2010 VMware, Inc. All Rights Reserved.
This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents
Exit

NOTE If the installation screen does not appear automatically or if you are installing from a network location, navigate to the root directory on the CD or share and double-click `setup.exe`.

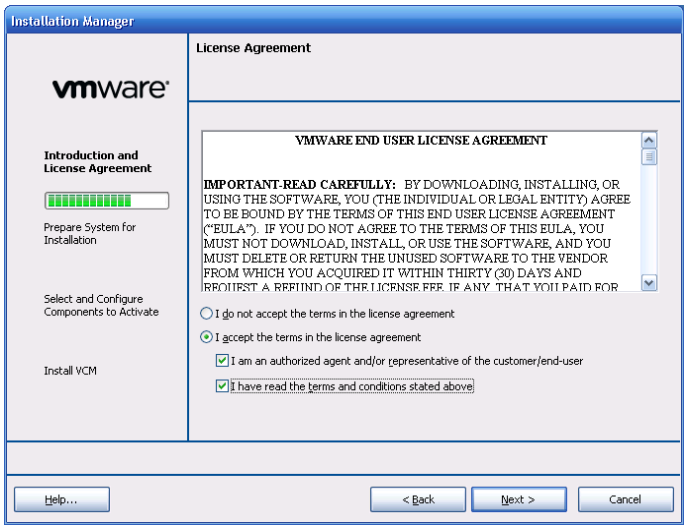
The installation screen provides the following options:

- **Run Installation Manager:** Launches Installation Manager.
- **View the Installation and Getting Started Guide:** Opens the *VCM Installation and Getting Started Guide*.
- **Browse Contents of Installation CD:** Launches Windows Explorer showing the contents of the root directory of the installation CD. You can navigate through the directory structure should you need to access documentation directly.
- **Contact Support:** Opens a pop-up dialog box that lists how to contact VMware Customer Support by e-mail and phone, including hours of operation.
- **Exit:** Exits Installation Manager and closes the installation screen.

2. Click **Run Installation Manager**. The **Introduction** page of the Installation Manager appears.


Installation Manager
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Introduction
Welcome to the Installation Manager
The Installation Manager will step you through the process of installing all the components. It will allow you to select the components you would like to activate.
Click Next to start the installation process.
Note:
Once you have installed and licensed the product, when you need to license additional components, access the License Manager node within Administration.
Help...
< Back
Next >
Cancel

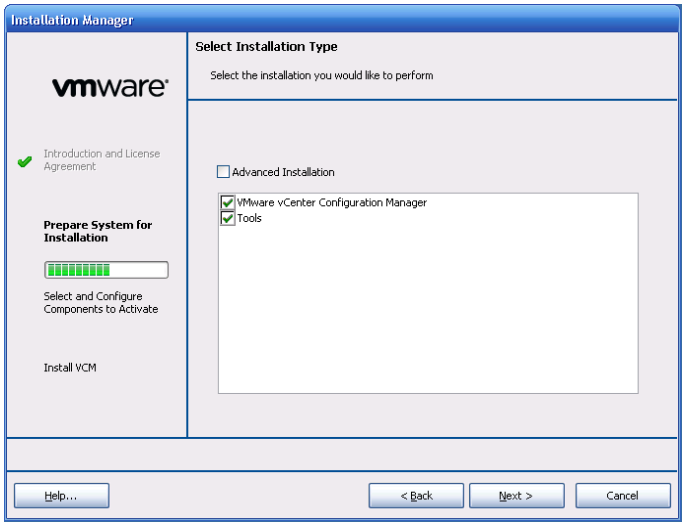
3. Click **Next**. The **License Agreement** page appears.


Installation Manager
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
License Agreement
VMWARE END USER LICENSE AGREEMENT
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND
I do not accept the terms in the license agreement
I accept the terms in the license agreement
I am an authorized agent and/or representative of the customer/end-user
I have read the terms and conditions stated above
Help...
< Back
Next >
Cancel

4. If you accept the terms explained on the License Agreement page, select the appropriate option and check boxes, and then click **Next**. The **Identify Available and Installed Components** page appears.

   It may take a few minutes for Installation Manager to identify which components are available for installation. During this time, the **Back** and **Next** buttons are inactive until Installation Manager finishes processing.

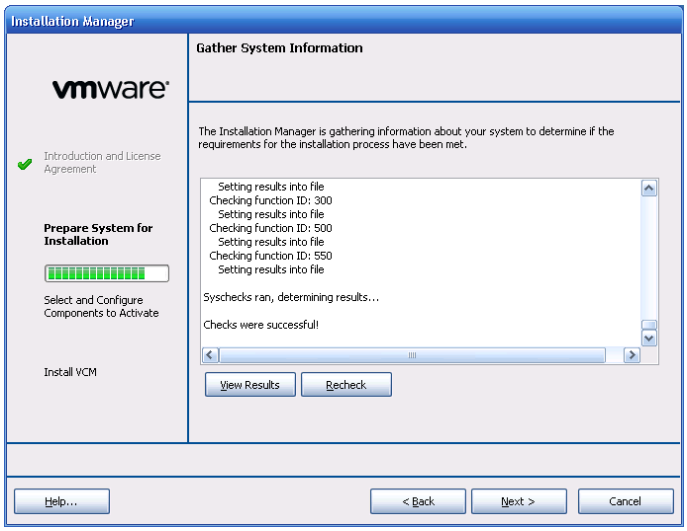
   When the evaluation process is completed, the **Select Installation Type** page appears.



5. When the **Select Installation Type** page first appears, the VMware vCenter Configuration Manager and Tools options are automatically selected.

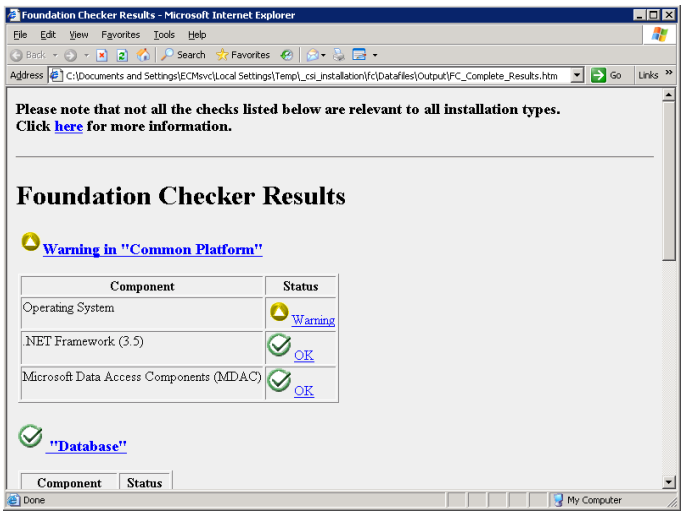
   To view all the components, select the **Advanced Installation** check box. The list expands to display the individual components. For a normal installation, all of the options should be selected.

   Click **Next**. The **Gather System Information** page appears.


Installation Manager
vmware
Gather System Information
The Installation Manager is gathering information about your system to determine if the requirements for the installation process have been met.
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Setting results into file
Checking function ID: 300
Setting results into file
Checking function ID: 500
Setting results into file
Checking function ID: 550
Setting results into file
Syschecks ran, determining results...
Checks were successful!
View Results
Recheck
Help...
< Back
Next >
Cancel

6. The **Gather System Information** displays the status of the Foundation Checker. The Foundation Checker reviews the machine's configuration and validates that the machine meets all the requirements for the installation. As Foundation Checker runs, various messages about the status of the check appear in the scrolling text box in the Gather System Information page.

- If the Foundation Checker detects missing or improperly configured settings, you are notified with the message "Errors detected". You will not be allowed to proceed with the installation until the errors are resolved. Click **View Results**. The **Foundation Checker Results** Web page appears. See the following example.
- If the Foundation Checker completes the validation successfully, you are notified with the message "Checks were successful!" and the **Next** button becomes active. Even though the checks were successful, VMware recommends you click the **View Results** button and read through the results to review any warnings that may represent potential issues for installation.



If you have only one or two errors, do not close the Installation Manager.

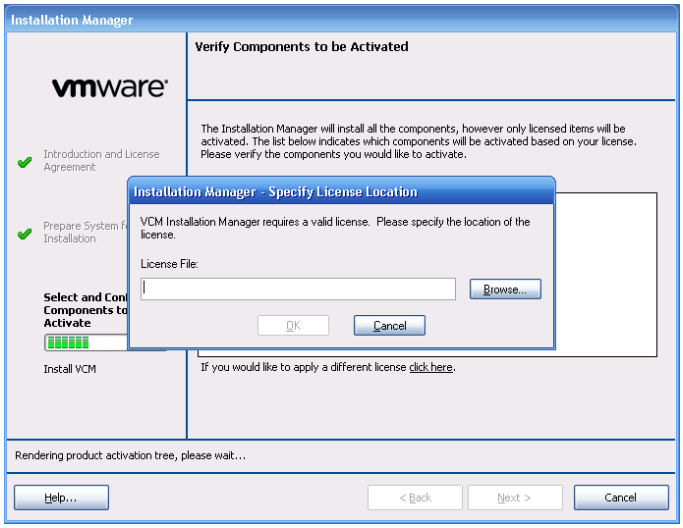
On the **Foundation Checker Results** Web page, review the Errors. Click the link associated with the errors you must resolve. A brief description is provided, along with a link to more detailed instructions for resolving the problem.

Refer to the *VCM Hardware and Software Requirements Guide* and the *VCM Foundation Checker User's Guide* for more information. If problems persist, contact VMware Customer Support.

If the fixes to the issues did not require a reboot, click **Recheck** on the **Gather System Information** page to restart the Foundation Checker process. If you are required to reboot the machine, you must start the installation process from the beginning.

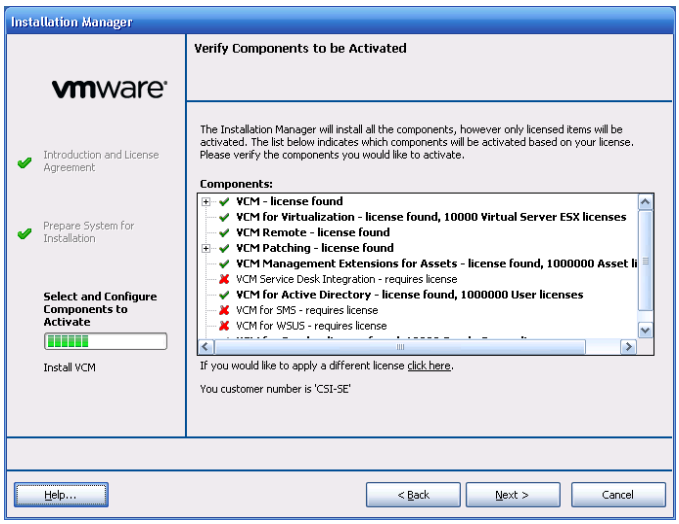
When the process completes successfully, "Checks were successful!" appears in the text box.

7. When the Foundation Checker process has completed successfully and you have viewed the results of the checking process, click **Next**. The **Specify License Location** dialog box appears in front of the **Verify Components to be Activated** page.


Installation Manager
Verify Components to be Activated
vmware
The Installation Manager will install all the components, however only licensed items will be activated. The list below indicates which components will be activated based on your license. Please verify the components you would like to activate.
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Installation Manager - Specify License Location
VCM Installation Manager requires a valid license. Please specify the location of the license.
License File:
Browse...
OK
Cancel
If you would like to apply a different license click here.
Rendering product activation tree, please wait...
Help...
< Back
Next >
Cancel

8. Click **Browse** to locate the license file provided by VMware. When you click **OK**, the **Verify Components to be Activated** page appears.

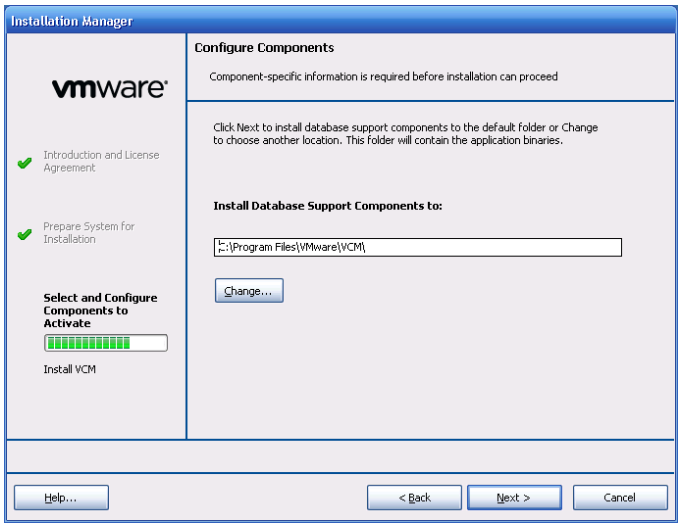
NOTE If you have not received your license file for VCM 5.3, contact your VMware Account Manager.


Installation Manager
Verify Components to be Activated
vmware
The Installation Manager will install all the components, however only licensed items will be activated. The list below indicates which components will be activated based on your license. Please verify the components you would like to activate.
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Components:
VCM - license found
VCM for Virtualization - license found, 10000 Virtual Server ESX licenses
VCM Remote - license found
VCM Patching - license found
VCM Management Extensions for Assets - license found, 1000000 Asset li
VCM Service Desk Integration - requires license
VCM for Active Directory - license found, 1000000 User licenses
VCM for SMS - requires license
VCM for WSUS - requires license
If you would like to apply a different license click here.
You customer number is 'CSI-SE'
Help...
< Back
Next >
Cancel

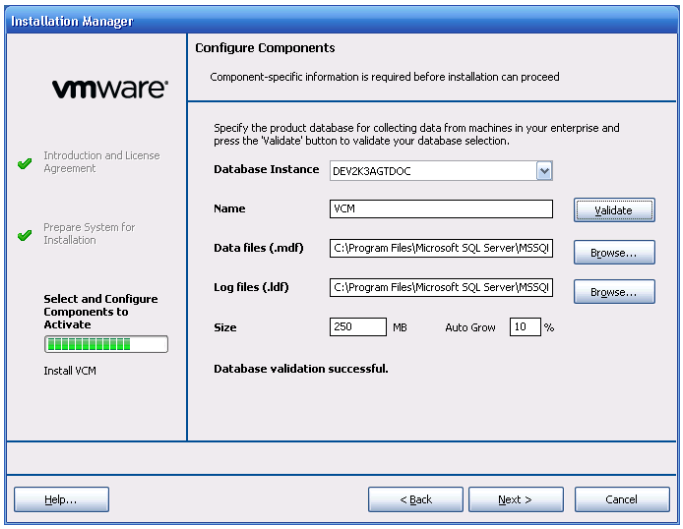
9. The **Verify Components to be Activated** page updates to display the components included in the license. Installation Manager installs VCM and all of its components on your machine. However, only the licensed components will be activated. Review the **Components** list to confirm the contents of your license file. If you applied an incorrect license file, click the link below the Components list and browse for a different file.

   If you have selected an invalid or expired license file, an error message will appear in a pop-up dialog box. Click **OK**, and the **VCM Specify License Location** dialog box appears, in which you can specify a valid license file.

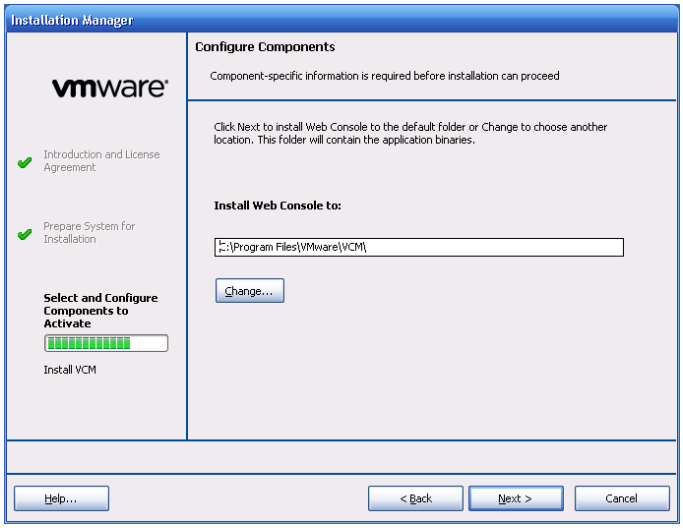
10. When you are ready to continue, click **Next**. The **Configure Components: Install Database Support Components to** page appears.


Installation Manager
Configure Components
Component-specific information is required before installation can proceed
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Click Next to install database support components to the default folder or Change to choose another location. This folder will contain the application binaries.
Install Database Support Components to:
C:\Program Files\VMware\VCM\
Change...
Help...
< Back
Next >
Cancel

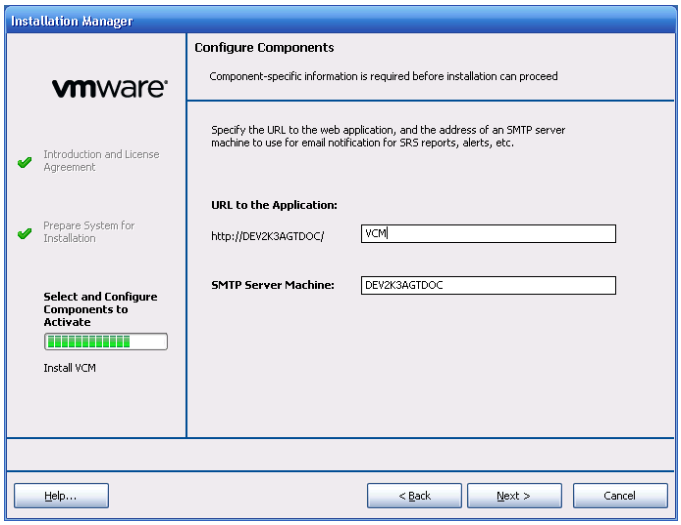
11. Specify the location for the VCM application files on the machine, and then click **Next**. The **Database Instance** and **Name** configuration page appears, where you will define the location for the VCM database.



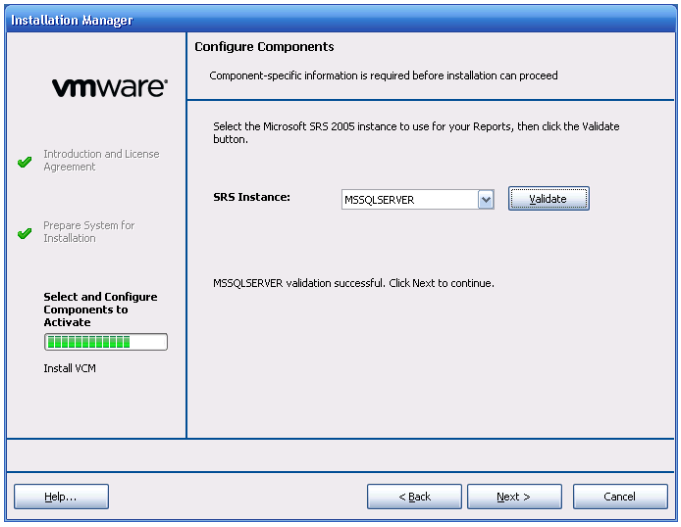
12. Specify the SQL Server instance and type a database name as needed. Click **Validate**. It could take a minute or two, and then the page updates to include the other SQL Server database settings.
13. Modify any file locations as needed, and then click **Next**. Most SQL database system administrators recommend that the Data files (.mdf) and the log files (.ldf) be placed on separate physical drives (spindles), and often require the files to be on a drive or partition other than the OS drive/partition. The **Install Web Console to** configuration page appears.


Installation Manager
vmware
Configure Components
Component-specific information is required before installation can proceed
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Click Next to install Web Console to the default folder or Change to choose another location. This folder will contain the application binaries.
Install Web Console to:
C:\Program Files\VMware\VCM\
Change...
Help...
< Back
Next >
Cancel

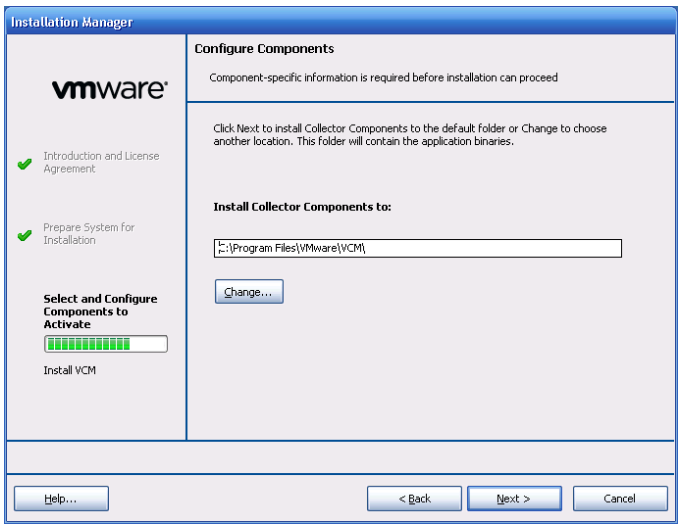
14. Specify the location if it is other than the default location, and then click **Next**. The **URL to the Application** configuration page appears.


Installation Manager
vmware
Configure Components
Component-specific information is required before installation can proceed
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Specify the URL to the web application, and the address of an SMTP server machine to use for email notification for SRS reports, alerts, etc.
URL to the Application:
http://DEV2K3AGTDOC/
VCM
SMTP Server Machine:
DEV2K3AGTDOC
Help...
< Back
Next >
Cancel

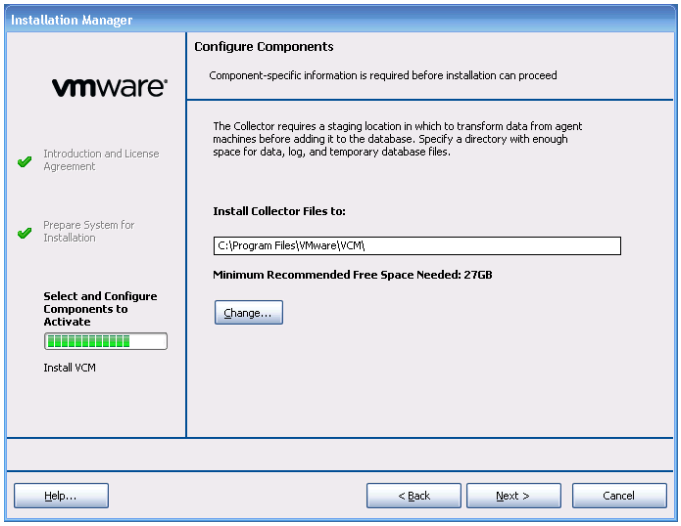
15. Change the values as needed, otherwise click **Next**. The **SRS Instance** configuration page appears.



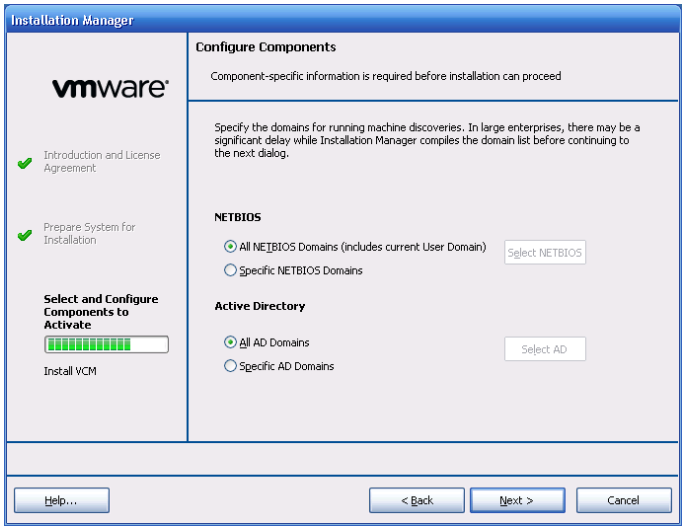
16. Click **Validate** and wait for the validation process to complete (it could take a minute or two). If the validation fails (for example, if the SSRS installation passed, but the foundation checks failed during the validation process), first verify that both "http://localhost/reports" and "http://localhost/reportserver" are accessible through a web browser. If that fails, stop the installation and call VMware Customer Support. The **Install Collector Components to** configuration page appears. When the validation process completes, click **Next**.


Installation Manager
vmware
Configure Components
Component-specific information is required before installation can proceed
Click Next to install Collector Components to the default folder or Change to choose another location. This folder will contain the application binaries.
Install Collector Components to:
C:\Program Files\VMware\VCM\
Change...
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Help...
< Back
Next >
Cancel

17. Change the path as needed, otherwise click **Next**. The page updates to display the option to specify a new location based on minimum space needs. Make any necessary changes. The **Install Collector Files to** configuration page appears.


Installation Manager
vmware
Configure Components
Component-specific information is required before installation can proceed
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
The Collector requires a staging location in which to transform data from agent machines before adding it to the database. Specify a directory with enough space for data, log, and temporary database files.
Install Collector Files to:
C:\Program Files\VMware\VCM\
Minimum Recommended Free Space Needed: 27GB
Change...
Help...
< Back
Next >
Cancel

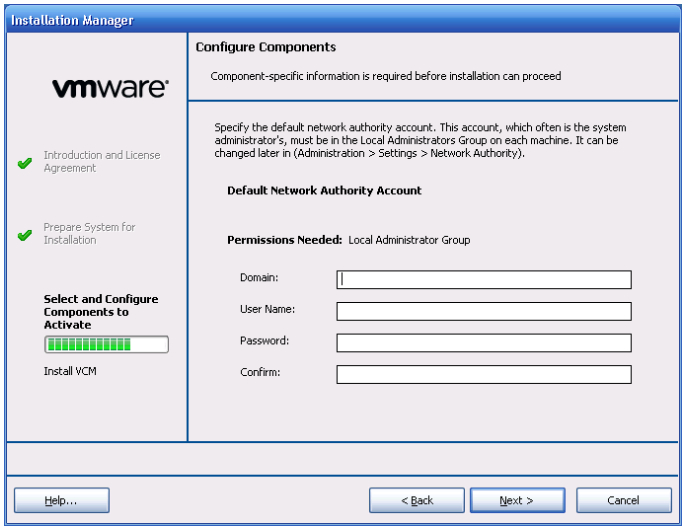
18. Change the path as needed, otherwise click **Next**. The **NetBIOS** and **Active Directory** configuration page appears.


Installation Manager
vmware
Configure Components
Component-specific information is required before installation can proceed
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Specify the domains for running machine discoveries. In large enterprises, there may be a significant delay while Installation Manager compiles the domain list before continuing to the next dialog.
NETBIOS
All NETBIOS Domains (includes current User Domain)
Specific NETBIOS Domains
Select NETBIOS
Active Directory
All AD Domains
Specific AD Domains
Select AD
Help...
< Back
Next >
Cancel

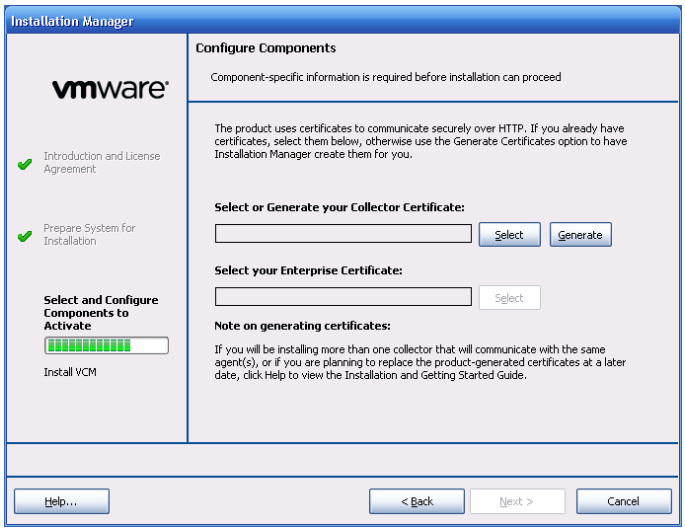
19. If you are managing only specific domains with this Collector, click the **Specific NetBIOS Domains** and **Specific AD Domains** options and configure as needed; otherwise, click **Next**. The **Default Network Authority Account** configuration page appears.

    At this point, you will need the Default Network Authority Account, Default Services Account, and Application Services Account. Additionally, you will need your Virtual Directory credentials if you intend to use VCM Remote.See "Checking Prerequisites for Installation" on page 13 for details.

    Only the **Default Network Authority Account** page is displayed below. The other Account pages have the same format but require different account information.


Installation Manager
Configure Components
Component-specific information is required before installation can proceed
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Specify the default network authority account. This account, which often is the system administrator's, must be in the Local Administrators Group on each machine. It can be changed later in (Administration > Settings > Network Authority).
Default Network Authority Account
Permissions Needed: Local Administrator Group
Domain:
User Name:
Password:
Confirm:
Help...
< Back
Next >
Cancel

20. Type the account information as specified in "Default Network Authority Account" on page 13, and then click **Next**. The **Default Collector Service Account** configuration page appears.
21. Type the account information as specified in "Default Collector Services Account" on page 14, and then click **Next**. The **Application Services Account** configuration page appears.
22. Type the account information as specified in "VMware Application Services Account" on page 14, and then click **Next**. The **Select or Generate your Collector Certificate** configuration page appears.


Installation Manager
Configure Components
Component-specific information is required before installation can proceed
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
The product uses certificates to communicate securely over HTTP. If you already have certificates, select them below, otherwise use the Generate Certificates option to have Installation Manager create them for you.
Select or Generate your Collector Certificate:
Select
Generate
Select your Enterprise Certificate:
Select
Note on generating certificates:
If you will be installing more than one collector that will communicate with the same agent(s), or if you are planning to replace the product-generated certificates at a later date, click Help to view the Installation and Getting Started Guide.
Help...
< Back
Next >
Cancel

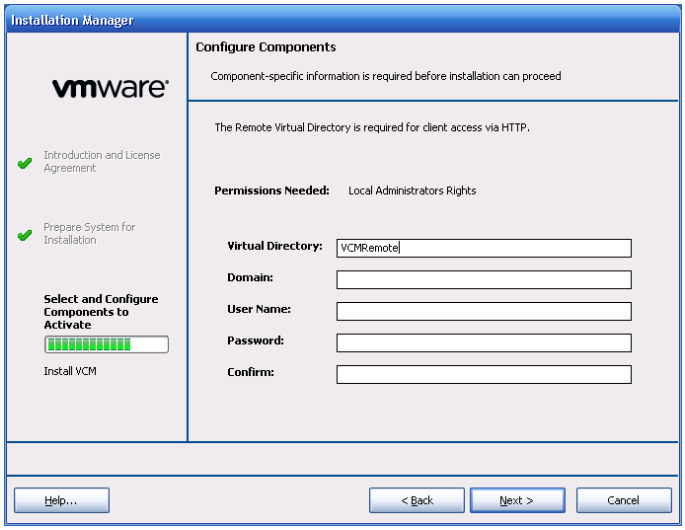
23. Select one of the following options:
    - **Select:** If you already have a pair of certificates with an established trust, click **Select** and then choose your certificates. All eligible certificates will be displayed in the Collector Certificate dialog. The Enterprise selection dialog is populated with certificates that are valid for the selected Collector Certificate.
    - **Generate:** If you do not have a pair of certificates with an established trust, click **Generate** to have Installation Manager generate the Collector and Enterprise certificates for you.

To specify a certificate different from the Collector certificate, click the **Select** button associated with **Select your Enterprise Certificate**. For more information about certificates, see "Secure Communications Certificates" on page 15.

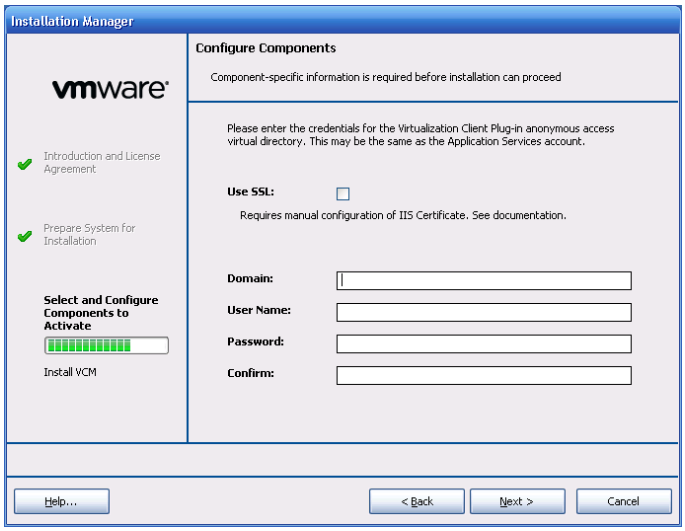
NOTE VCM does not allow apostrophes in TLS certificate names. Before selecting a certificate, verify that the name does not contain an apostrophe.

IMPORTANT If you will be installing more than one Collector that will communicate with the same Agent(s), or if you plan to replace/renew your certificates at a later date, there are special considerations for generating and selecting certificates in Installation Manager. For more information about VCM and TLS, see the *Transport Layer Security (TLS) Implementation for VCM* white paper located on the VMware vCenter download site.

24. Click **Next**. The **Remote Virtual Directory** configuration page appears.



25. Enter the account information as specified in "VCM Remote Virtual Directory" on page 14, and then click **Next**. The vSphere Client VCM Plug-in (VCVP) configuration page appears.

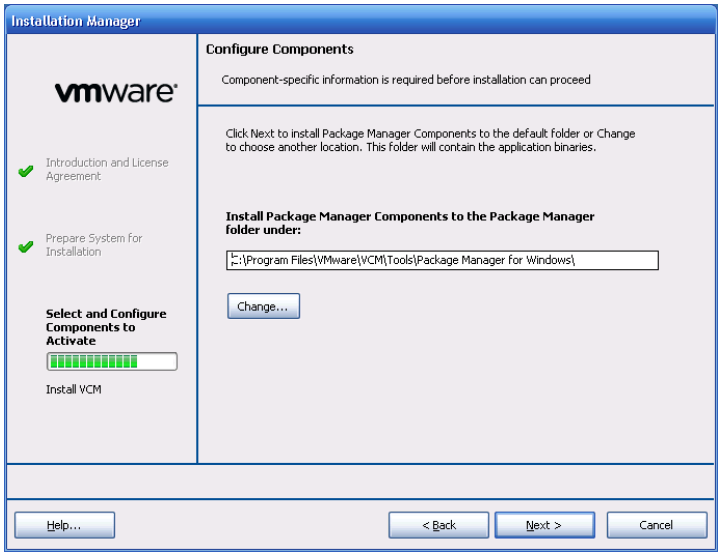

Installation Manager
Configure Components
Component-specific information is required before installation can proceed
vmware
Please enter the credentials for the Virtualization Client Plug-in anonymous access virtual directory. This may be the same as the Application Services account.
Introduction and License Agreement
Use SSL:
Requires manual configuration of IIS Certificate. See documentation.
Prepare System for Installation
Domain:
Select and Configure Components to Activate
User Name:
Password:
Install VCM
Confirm:
Help...
< Back
Next >
Cancel

26. The vSphere Client VCM Plug-in (VCVP) provides VMware vSphere Client users with the ability to Collect, Run Compliance, Run VCM Patching Assessments, and Run Reports on VM Hosts and Guests.

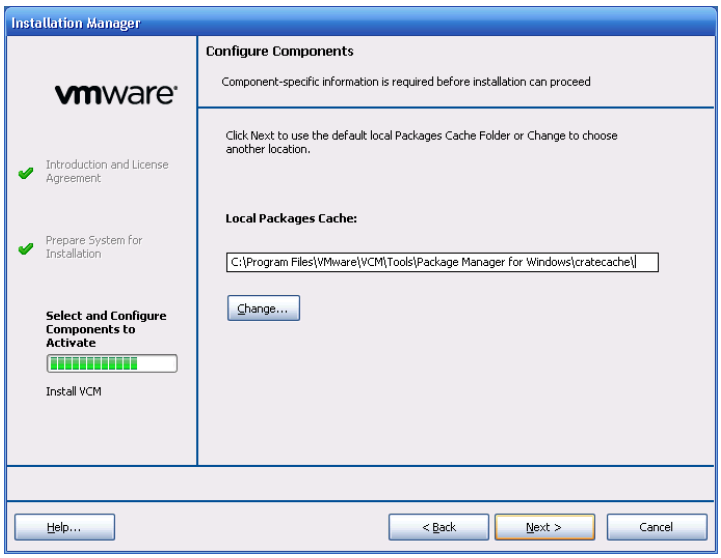
    To configure the settings:

    - Select **Use SSL** only if you configured the machine for SSL.
    - Whether you are using SSL or not, you should define the user name and password at this time. The credentials provided here are similar to the credentials used for Application Services, providing client access using HTTP.

27. Click **Next**. The **Install Package Manager Components to the Package Manager folder under** page appears.

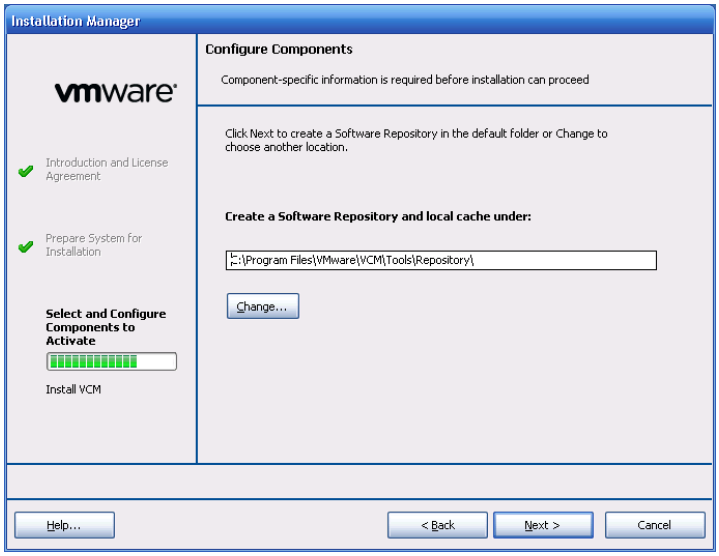

Installation Manager
Configure Components
Component-specific information is required before installation can proceed
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Click Next to install Package Manager Components to the default folder or Change to choose another location. This folder will contain the application binaries.
Install Package Manager Components to the Package Manager folder under:
C:\Program Files\VMware\VCM\Tools\Package Manager for Windows\
Change...
Help...
< Back
Next >
Cancel

28. Package Manager Components will be installed in order to support Software Provisioning functionality, including installing and removing packages. Either change the path or click **Next**. The **Local Packages Cache** page appears.

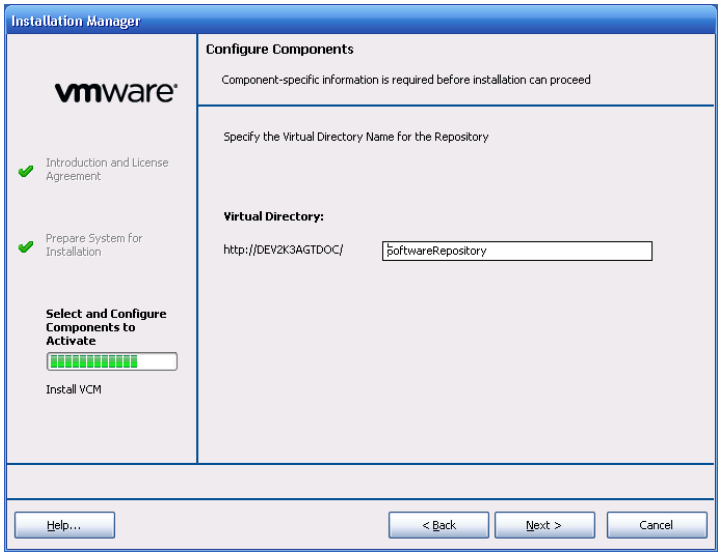

Installation Manager
Configure Components
Component-specific information is required before installation can proceed
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Click Next to use the default local Packages Cache Folder or Change to choose another location.
Local Packages Cache:
C:\Program Files\VMware\VCM\Tools\Package Manager for Windows\cratecache\
Change...
Help...
< Back
Next >
Cancel

29. The Packages Cache Folder is used by Software Provisioning to store packages that have been

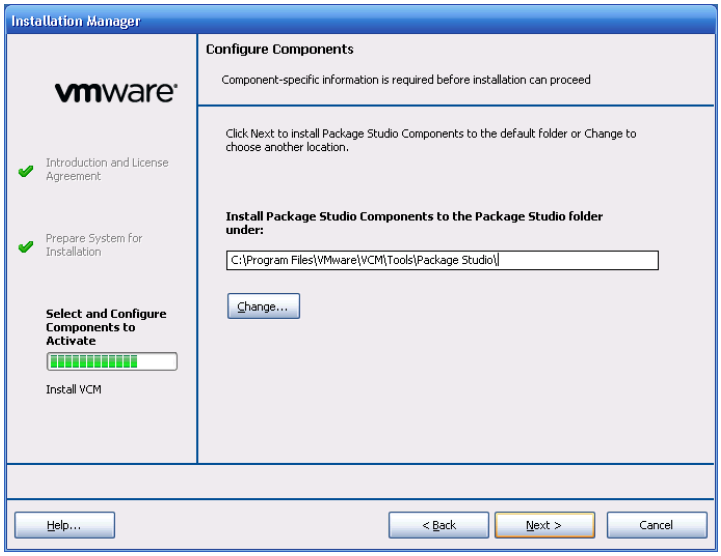
downloaded. Either change the path or click **Next**. The **Create a Software Repository and local cache under** page appears.


Installation Manager
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Configure Components
Component-specific information is required before installation can proceed
Click Next to create a Software Repository in the default folder or Change to choose another location.
Create a Software Repository and local cache under:
C:\Program Files\VMware\VCM\Tools\Repository\
Change...
Help...
< Back
Next >
Cancel

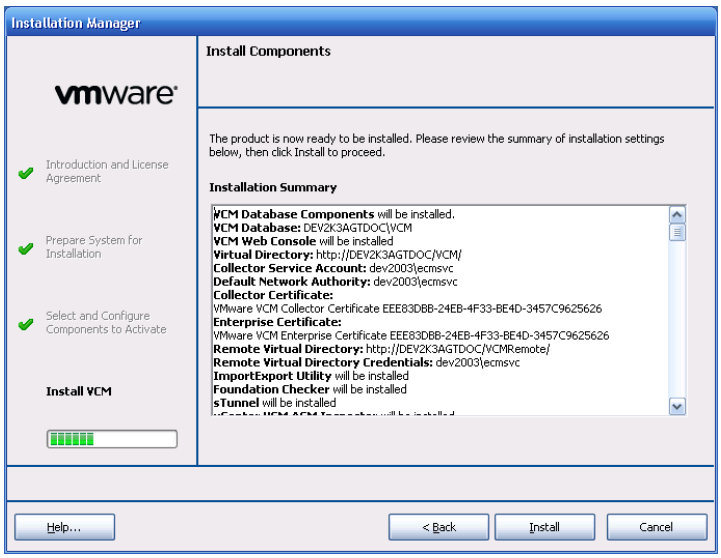
30. The Software Repository is used by Software Provisioning as a location to store packages for distribution to other systems. Either change the path or click **Next**. The **Virtual Directory** page for the Software Repository appears.



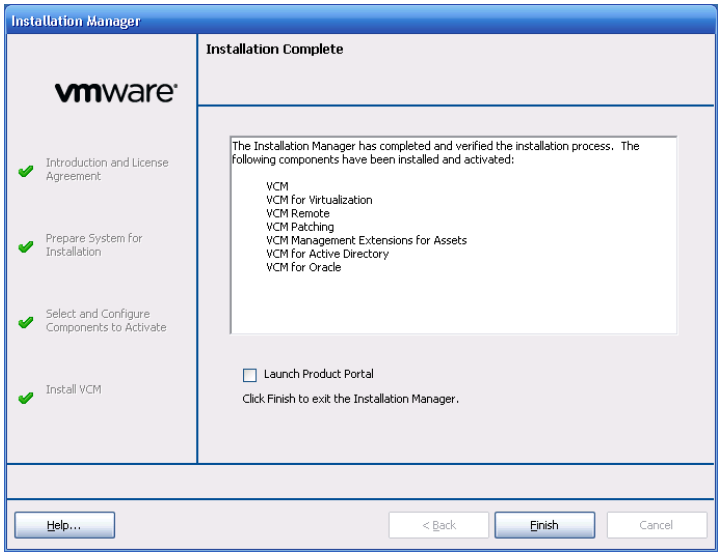
31. Enter a name for the virtual directory, and then click **Next**. The **Install Package Studio Components to the Package Studio folder under** page appears.


Installation Manager
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Configure Components
Component-specific information is required before installation can proceed
Click Next to install Package Studio Components to the default folder or Change to choose another location.
Install Package Studio Components to the Package Studio folder under:
C:\Program Files\VMware\VCM\Tools\Package Studio\
Change...
Help...
< Back
Next >
Cancel

32. Package Studio Components will be installed in order to support Software Provisioning functionality, including creating and publishing packages. Either change the path or click **Next**. The **Installation Summary** page appears.


Installation Manager
vmware
Introduction and License Agreement
Prepare System for Installation
Select and Configure Components to Activate
Install VCM
Install Components
The product is now ready to be installed. Please review the summary of installation settings below, then click Install to proceed.
Installation Summary
VCM Database Components will be installed.
VCM Database: DEV2K3AGTDOC\VCM
VCM Web Console will be installed
Virtual Directory: http://DEV2K3AGTDOC/VCM/
Collector Service Account: dev2003\ecmsvc
Default Network Authority: dev2003\ecmsvc
Collector Certificate:
VMware VCM Collector Certificate EEE83DBB-24EB-4F33-BE4D-3457C9625626
Enterprise Certificate:
VMware VCM Enterprise Certificate EEE83DBB-24EB-4F33-BE4D-3457C9625626
Remote Virtual Directory: http://DEV2K3AGTDOC/VCMRemote/
Remote Virtual Directory Credentials: dev2003\ecmsvc
ImportExport Utility will be installed
Foundation Checker will be installed
sTunnel will be installed
Help...
< Back
Install
Cancel

33. Wait for the components to be installed. The **Installation Complete** page appears.



34. When the installation completes, you can select the **Launch Product Portal** option to start VCM after you click **Finish**.

35. Review the displayed information. If it is incorrect, click **Back** and make any necessary changes. If it is correct, click **Install**. The installation process begins. A status bar displays the process stages until the installation is completed, at which time the **Installation Complete** page appears.

NOTE Depending upon your hardware configuration, the installation process for a new installation may take 30 minutes or longer to complete.

If Installation Manager encounters an irrecoverable installation error, a message to this effect appears in a pop-up dialog box, with a path to the installation log where you can view information about the error. When you click **OK**, both the pop-up dialog box and Installation Manager close. In this case, read the information about the error in the installation log, capture the log, and contact the VMware Customer Support before proceeding.

36. To open VCM, select **Launch Product Portal**, and then click **Finish**.

NOTE VMware recommends that you take the time to configure SQL Server settings now, including configuring the database file growth and database recovery settings, in order to fine-tune your VCM Database. Instructions for configuring these settings are provided in "Maintaining VCM After Installation" on page 247.

CAUTION As part of installation, a folder containing VCM-related .msi files is added to `%windir%\Installer\`. If the contents of this folder are moved or deleted, you will be unable to successfully upgrade, repair, or uninstall using the VCM Installation Manager.

Upgrading VCM and Related Components 3

This chapter provides important information that will help you upgrade VCM and the tools in your enterprise. This chapter describes the following:

- Upgrading to VCM 5.3.0
- Upgrading Existing UNIX Agents
- Upgrading VCM for Virtualization
- Upgrading VCM Reports

Prerequisites

VCM provides support for 64-bit systems (64-bit hardware and 64-bit operating system), and SQL Server 2005. If you intend to move from a 32-bit environment to a 64-bit environment, you must prepare your 64-bit environment for a VCM installation by following the instructions in this chapter.

For information about configuring a 64-bit machine as a Collector, see the VCM Hardware and Software Guide.

Before upgrading to VCM 5.3.0, your version of VCM must be 4.11.1 or later.

CAUTION Before Installing VCM 5.3.0 on a 32-bit System, check for the following registry entry, and rename or remove it if it exists: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node`. VCM 5.3.0 uses this registry entry to detect whether the system is a 32-bit or 64-bit operating system.

Backup and Recovery

CAUTION Before starting any VCM upgrade, be sure to back up your databases and file system.

The upgrade may be from SCM to VCM or VCM to VCM. If you are upgrading VCM, the databases to back up include the following: CSI_Domain, VCM, VCM_Coll, VCM_UNIX, ReportServer, master, and msdb.If you are upgrading SCM to VCM, the databases to back up include the following: CSI_Domain, SCM, SCM_Coll, SCM_UNIX, ReportServer, master, and msdb.

The file system to back up is the entire contents of the CMFILES$ share. The default location is C:\Program Files\VMware\VCM\WebConsole\L1033\Files\. If customizations have been made to your collector, or if reports have been exported to a non-default location, you must also ensure that these additional files are backed up.

To recover if the upgrade process is unsuccessful, reinstall the version from which you were upgrading, reconnect the databases from the back up copies, and replace the CMFILES$ share files. Contact VMware Customer Support to assist with identifying possible causes for the unsuccessful upgrade process before again attempting the upgrade.

Assumptions for Upgrading Your VCM Collector and Database

- Your current installation is functional.
- Your customer number is consistent throughout the upgrade process.
- All running jobs have completed, and no jobs are scheduled to start during the upgrade process. The upgrade will stop the SQLAgent service. This will cancel any running jobs and prevent new jobs from starting.
- All users are logged off and will not be accessing VCM for the duration of the upgrade process.

If you have any questions regarding these procedures, contact VMware Customer Support before proceeding.

Upgrading to VCM 5.3

The upgrade from VCM 4.11.1 or later to 5.3 supports installation of the VCM Collector with the following:

- 32-bit hardware running Windows Server 2003 SP2 32-bit, with SQL Server 2005 32-bit
- 64-bit hardware running Windows Server 2003 SP2 64-bit, with SQL Server 2005 64-bit and 32-bit SQL Server Reporting Services
- Microsoft SQL Server 2005

CAUTION Before upgrading, be sure to back up your database(s) to avoid any potential loss of data.

Upgrading the VCM Database Only

To "upgrade" an existing VCM database (4.11.1 or later), move the database to a 64-bit SQL Server, attach it to SQL Server, and then install VCM.

Upgrading VCM on a 32-Bit System

If you are using a version of VCM prior to 4.11.1, such as version 4.9.1 which uses SQL 2000, when upgrading on a 32-bit system (32-bit hardware and a 32-bit operating system), you must upgrade SQL Server 2000 to SQL Server 2005, including Reporting Services (32-bit only), and then install SQL Server 2005 SP3.

You must then upgrade to VCM 4.11.1 by following the upgrade documentation for that version, and then upgrade to VCM 5.3.

Upgrading to a 64-Bit System

When upgrading to a 64-bit system (64-bit hardware and a 64-bit operating system), you must install 64-bit SQL Server 2005 and SP3. You must also install, update, and configure 32-bit SQL Server Reporting Services (SSRS). After installing the 32-bit version of SSRS, you must also install the 32-bit SSRS SP3.

When upgrading to a 64-bit system, during the upgrade process you will:

1. Detach a VCM 4.11.1 or newer database that is running in a 32-bit system.
2. Copy the VCM database to a 64-bit machine that is running the 64-bit version of SQL Server 2005.
3. Attach the existing VCM 4.11.1 or newer database to SQL Server.
4. Install VCM 5.3.

Because versions of VCM prior to 4.11.1 cannot be installed on a 64-bit platform, you will not be upgrading VCM on a 64-bit platform.

Before Upgrading

Before upgrading to VCM 5.3, make sure that you have already installed the following components, as described in the *VCM Hardware and Software Requirements Guide*.

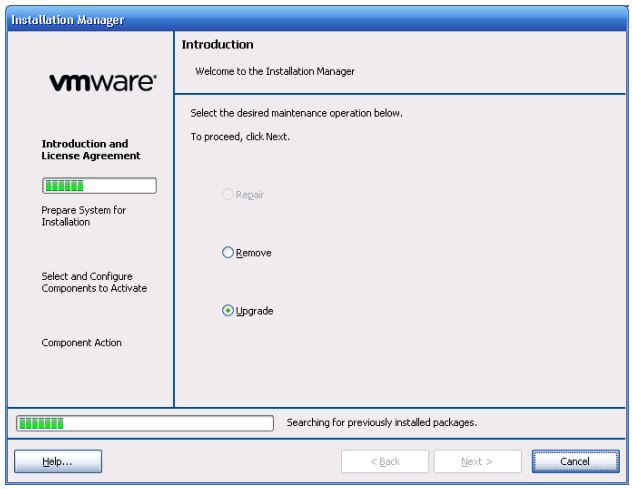
- VCM 4.11.1 or later.
- The required versions of the Microsoft .NET Framework. See the *Hardware and Software Requirements Guide* for details.
- **For 32-bit systems:** SQL Server 2005, and then install SQL Server 2005 SP3.
- **For 64-bit systems:** 64-bit SQL Server 2005 and SQL Server 2005 SP2, **and** 32-bit SQL Server Reporting Services and SSRS SP3.

NOTE When the installation of these software packages is complete, the VCM Foundation Checker results should be successful. If errors still occur, resolve them using the built-in Help and the *VCM Hardware and Software Requirements Guide*.

Performing the Upgrade

Use the following procedure to upgrade from VCM 4.11.1 or later to VCM 5.3.

1. Start the upgrade from the VMware vCenter download site or the CD, and select the **Upgrade** VCM option.



The **Upgrade**, **Uninstall**, and **Repair** options are available as follows:

- **Installing directly:** When running the installation `setup.exe` file directly, options to **Upgrade** and **Remove** (uninstall) VCM are available.

- **Installing using Add/Remove Programs:** When invoking `setup.exe` from Add/Remove Programs, the option to repair VCM is available. The **Repair** option checks for missing files and settings, and then replaces them.

CAUTION You should not invoke Repair unless directed to do so by VMware Customer Support. Repair requires access to your original installation media.

---

2. Click **Next**. The **License Agreement** page appears.
3. Review and accept the license agreement, and then click **Next**. The **Select Installation Type** page appears.
4. Ensure that all of the components are marked for installation.

NOTE If one of the software components cannot be upgraded, the check box for the specified component will be cleared and a note will be added next to the node in the selection dialog indicating why it is disabled. This situation can occur due to an invalid upgrade or an incomplete copy of the install image.

---

5. Click **Next**. The **Gather System Information** page appears.
6. Foundation Checker will gather information about the machine to prepare it for the installation. When the system check is complete, the Foundation Checker results will either be successful or show errors. For the upgrade to proceed, the results must be successful. If the system checks encounter errors, you must resolve those errors before proceeding. Click **View Results** and use Foundation Checker Help to locate the source of the problem.
7. After the system checks are successful, Installation Manager displays a summary of the components to be installed. To continue, click **Next**. The **Configure Components** page appears, requesting confirmation of the **Default Collector Service Account**.
8. If the account is changing, type the new values. If the account remains the same, click **Next**. The **Application Services Account** configuration page appears.
9. If the account is changing, type the new values. If the account remains the same, click **Next**. The **CM Remote Virtual Directory** configuration page appears.
10. If the account is changing, type the new values. If the account remains the same, click **Next**. The **Virtualization Client Plug-in** configuration page appears.
11. Do not select SSL unless your machine is already configured for SSL.
12. If the account is changing, type the new values. If the account remains the same, click **Next**. The **Install Components** page appears.
13. Review the summary list, and then click **Upgrade**. The installation process begins. Depending on your hardware configuration, the process may take 30 minutes or longer.
14. When the process is completed, the **Upgrade/Repair Complete** page appears.
15. When the Installation Manager has successfully upgraded the software components, click **Finish**.

NOTE VMware strongly recommends that you take the time to configure SQL Server settings now, including configuring the VCM database file growth and database recovery settings, in order to fine-tune your VCM Database. Instructions for configuring these settings are provided in "Maintaining VCM After Installation" on page 247.

Upgrading Existing Windows Agents

Use the Upgrade Agent wizard to upgrade the Agent files on one or more machines.

To upgrade an Agent:

1. Click **Administration** | **Machines Manager** | **Licensed Machines** | **Licensed Windows Machines**.
2. Select the machine or machines you are upgrading, and then click the **Upgrade Agent** icon on the Licensed Windows Machines toolbar. The Machines page appears.
3. Select a machines option.

Option	Definition
All machines	Upgrade the Agent on all machines that appear in the list of licensed machines.
Filtered machines only	This option is available only if the Licensed Machines list is being filtered. Upgrade the Agent on all machines that appear in the filtered list of machines.
Selected machine(s) only	Upgrade the Agent only on select individual machines. Use the standard selection method to select individual machines.

4. Click **Next**. The **Install Options** page appears.
5. In the **Install From** field, select or verify the necessary information.

   The default source of the Agent files is the Collector machine. If you have created an Alternate Source, you can select it from the drop-down list.

   The Upgrade process:

   - Will fail for any machine on which an Agent does not already exist.
   - Will use an Agent's current settings. For example, if the Agent uses DCOM, the Upgrade will maintain that setting. If the Agent uses HTTP on Port 1024, the Upgrade will maintain that setting.
   - Will not upgrade components that do not require upgrading.
6. Click **Next**. The **Schedule** page appears.
7. Schedule the operation. You can enter the Date in the specified format, or click the Calendar icon.
8. Click **Next.** The **Important** page appears.
9. Verify the actions that will be performed and then click **Finish**.

Upgrading Existing Remote Clients

VMware recommends that you upgrade your Remote client versions. When the automatic upgrade setting (**Will Remote automatically upgrade old Remote clients**) is set to **Yes**, the next client-server contact automatically downloads and install the upgrade files.

If the Remote client does not have a certificate, the upgrade process will automatically extract the certificate and send it to the client, along with the new Agent.

To automatically upgrade your remote clients:

1. Click **Administration | Settings | General Settings | VCM Remote**.
2. Select **Will Remote automatically upgrade old Remote clients.**
3. Click **Edit Setting**. The **Edit Setting** wizard appears.
4. Change the setting to **Yes**.
5. Click **Next**. The confirmation page appears.
6. Click **Finish**. The setting change is saved.

Upgrading Existing UNIX Agents

Upgrade packages are available to update the UNIX Agents on various platforms. To upgrade the UNIX Agents to the latest software release, use one of the following methods:

- Upgrade the UNIX Agent(s) with the Local Package
- Upgrade the UNIX Agent(s) with a Remote Package

VCM supports TLS for UNIX/Linux. For more information, see TLS Implementation for VCM, posted on the VMware vCenter download site.

If you are installing on HP-UX 11.11, Patch PHSS_30966 is required for the HP-UX Agent. If you need assistance, contact VMware Customer Support.

Upgrading Red Hat Workstations

In previous versions of VCM, Red Hat machines, either workstations or servers, were licensed as Red Hat servers. Beginning with version 5.2.0, Red Hat machines were licensed as either workstations or servers. When you upgrade to 5.2.0 or later, the workstations, previously managed with a server licenses, will be unmanaged in VCM. The unmanaged Red Hat workstations should be listed in the Available UNIX Machines list. To manage the machines in VCM, go to Administration | Machines Manager | Available Machines | Available UNIX Machines and re-license the machines using Linux/Mac Workstation licenses.

If you are unable to identify your now unmanaged Red Hat machines, contact VMware Customer Support.

Platforms Not Supported for Upgrade to 5.3 Agent

Installing or upgrading on the following platforms is supported only to the 5.1.3 UNIX Agent. You can install the 5.3 Agent; however these platforms are not tested with any additional 5.3 functionality.

Platform	Supported Agent Version	Agent File Name
AIX 4.3.3	5.1.3	CMAgent.5.1.0.AIX.4
Red Hat 2.1	5.1.3	CMAgent.5.1.0.Linux.2.1
Solaris 2.5	5.1.3	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.
Solaris 2.6	5.2.1	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.

To Upgrade the UNIX Agent(s) with a Local Package

To upgrade the UNIX Agent(s) using the local upgrade package, follow these steps:

1. Locate the AgentUpgradeLocal.sh file in `\Program Files\VMware\VCM\WebConsole\L1033\Files\UNIX_Remote_Command_Files`.
2. Open the `AgentUpgradeLocal.sh` file with a text editor like Wordpad.
3. In the AgentUpgradeLocal.sh file, locate the following entry:
   `CSI_INSTALL_PACKAGE_LOCATION = CHANGE_THIS_TO_A_LOCAL_OR_NFS_DIRECTORY`
4. Change this entry to point to either a local directory or an NFS directory where the VCM Agent Install Packages are located (for example, `/tmp/VCMu_Agent`).

   NOTE Agent install packages are installed on the Collector machine at `\Program Files\VMware\VCM\Installer\Packages`.

5. Save and close the `AgentUpgradeLocal.sh` file.
6. Log into VCM and open the Console slider. Navigate to **Console | UNIX Remote Commands | UNIX Agent Upgrade**. The UNIX Agent Upgrade data grid appears.
7. Select **Agent Upgrade - Local Package**.
8. Click **Run**. The Remote Commands wizard appears.
9. Select the machine(s) on which you want to upgrade the agent.

   NOTE To determine which Agent is currently on a UNIX machine, navigate to **Administration | Machines Manager | Licensed Machines | Licensed UNIX Machines**. To determine the latest version number for the Agent, select **About | Versions**.

10. Click the arrow button to move the machines from the **Available list** to the **Selected list**. Click **Next**.
11. Select whether you want to upgrade the Agent now or later. To change the date, click the **Calendar** icon. When you schedule the action, it is placed in the **Administration | Job Manager | Scheduled** list.

    NOTE The Time of Day settings you choose are based on your User time zone. All VCM jobs run based on the VCM Database time zone. You must account for the time and date differences between your VCM User time and your VCM Database time. For example, if your VCM Database server is in the Eastern time zone, and your VCM User is in the Pacific time zone, to run your job at midnight, you would enter 9 PM.

12. Click **Next**, and then click **Finish**.

To Upgrade the UNIX Agent(s) with a Remote Package

This method sends the upgrade package with the remote command to execute on the UNIX machine. The following remote upgrade packages are designed specifically for the various operating systems where the Agent(s) can be upgraded:

- AIX 4.3.3 Agent Upgrade (use only CMAgent.5.1.0.AIX.4)
- AIX 5 Agent Upgrade
- HP-UX (Itanium) Agent Upgrade

- HP-UX (PA-RISC) Agent Upgrade
- Red Hat Enterprise 2.1 Agent Upgrade (use only CMAgent.5.1.0.Linux.2.1)
- Red Hat Enterprise 3.0, 4.0, 5.0, 5.1, 5.2, SUSE Enterprise 9 and above Agent Upgrade
- Solaris (SPARC) Agent Upgrade
- Solaris (x86) Agent Upgrade

To upgrade the UNIX Agent(s) using one of the remote upgrade packages, follow these steps:

1. Navigate to **Console | UNIX Remote Commands | UNIX Agent Upgrade**. The UNIX Agent Upgrade data grid appears.
2. Click to highlight the remote upgrade package that is appropriate for the operating system and version of the machine(s) that you want to upgrade.
3. Click Run and follow the wizard instructions to send the remote command and the upgrade package to the Agent(s) on the selected machine(s). The Agent will then execute the upgrade package.

The UNIX Agents are now using TLS, therefore the Enterprise Certificate is embedded in the Agent package. If multiple Collectors need to talk to a single Agent, then all of the Collectors should share an Enterprise Certificate. If the Collectors have different Enterprise Certificates, then the Enterprise Certificate from each Collector must be uploaded to the Agent. For more information, see TLS Implementation for VCM, located on the VMware vCenter download site.

Upgrading VCM for Virtualization

When upgrading a Collector to VCM 5.3, the Agent Proxy is automatically upgraded, and the Agent Proxy protected storage and user account configuration settings are preserved. However, for existing non-Collector Agent Proxy machines, you must upgrade VCM for Virtualization, and select to retain the Secure Communication settings.

To upgrade the VCM for Virtualization Agent Proxy on non-Collector machines, you must use one of these methods, depending on your configuration:

- Manually Upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine
- Use VCM to Upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine

---

CAUTION When upgrading VCM for Virtualization, take the following precautions:

Do not change the password for the CSI Communication Proxy service. Doing so may require the Agent Proxy to be reinstalled and reconfigured.

Avoid installing the Agent Proxy and the Active Directory product on the same machine. The operations involved to install, uninstall, upgrade, and reinstall these products may result in the Agent Proxy needing to be reinstalled and reconfigured.

If you plan to uninstall VCM for Virtualization manually, make sure that you execute RetainSecureCommSettings.exe before uninstalling it. Otherwise, the Agent Proxy configuration settings will be removed, and the Agent Proxy will need to be reconfigured. The RetainSecureCommSettings.exe is located at: C:\Program Files\VMware\VCM\Installer\Packages, or in the path relative to where you installed the software.

Platform Not Supported for Upgrade to 5.3 Agent Proxy

You can install or upgrade an Agent Proxy machine only to the 5.1.3 Agent if it is collecting from this platform. This platform is not tested with the 5.3 functionality.

Platform	Supported Agent Version	Agent File Name
ESX 2.5	5.1.3	

Upgrading an Agent Proxy Machine

If a new version of the Agent Proxy becomes available, the upgrade process installs the newer version on your agent proxy machine.

1. Click **Administration | Machines Manager | Additional Components | VCM for Virtualization | Agent Proxies**. The **Agent Proxies** data grid appears.
2. Select the machine or machines on which you are upgrading the Agent Proxy.
3. Click **Upgrade**. The **Machines** page of the **Upgrade Agent Proxies** wizard appears.
4. The available machines are displayed in the upper list. The selected machines are displayed in the lower list. You can perform the following actions on the page:
   - **All Machines:** Select the option to run the process on all eligible machines.
   - **Selected Machines Only:** (Default option) Select the option to run the process on all machines listed in the lower pane.
   - **Filtered Machines:** Click **Define** to create a filter based on Machine Name or Domain Name, and then select the Filtered Machines option.
   - **Arrow buttons:** Select a machine name in one of the panes and use the arrow buttons to move it from one pane to the other. Additionally, you may double-click a machine name to move it between panes.
5. Click **Next**. The **Option** page appears.
6. Configure the following options:
   - **Install From:** In the drop-down list, select the name of the Collector used to manage virtual machines.
   - **Schedule:** Select **Run Action now** to install immediately, or select **Schedule the Action to run later** and configure the settings to run at a designated time.
7. Click **Next**. The **Important** page appears. Review the contents, click **Back** to make any necessary alterations.
8. Click **Finish**. The Agent Proxy is upgraded at the time specified.
9. To verify the completion of the upgrade process, click **Jobs** on the Portal toolbar to access the Jobs Summary. You can also verify jobs for the past 24 hours if you think that you may have missed it. Go to **Administration | Job Manager | History | Other Jobs | Past 24 Hours**.

Manually Upgrading an Agent Proxy Machine

The steps provided in this section are an optional upgrade method if you choose not to use the Upgrade option in VCM. To manually upgrade an Agent Proxy machine, you must have already upgraded your Collector machine to VCM 5.3. Then you will uninstall the VCM Agent, select to retain the Secure Communication settings, install the VCM Agent (version 5.3), and then install VCM for Virtualization, as described in the following steps.

1. The following executable must be accessible from your non-Collector Agent Proxy Machine. The path to this file on the Collector machine is as follows, or is in the path relative to where you installed the software.

   ```
   C:\Program Files\VMware\VCM\AgentFiles\CMAgentInstall.exe
   ```

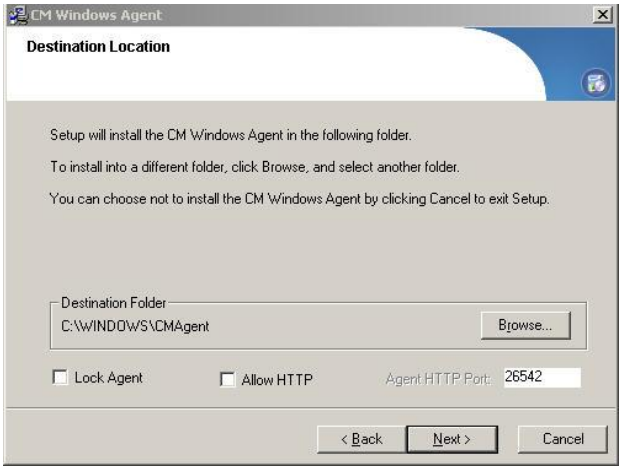
   Then execute the copied `CMAgentInstall.exe` on your Agent Proxy machine.

2. The installer detects the previous version of VCM, and then requests permission to uninstall it. Select **Yes**.

3. The installer detects that Secure Communication is installed, and requests whether you want to retain your settings. Select **Yes**. The installer proceeds to remove the VCM Virtualization product and VCM Agent from your Agent Proxy machine. During this process, your Secure Communication settings are retained.

4. When the installer displays the license agreement, read and then accept the conditions.

5. The installer prompts whether to perform the installation of the VCM Windows Agent in HTTP mode. Allowing HTTP communication will allow the Agent to communicate through the HTTP port specified if DCOM is not available. Locking an Agent will prevent the Agent from being removed or upgraded. To use this mode, select **Allow HTTP**, and click **Next**.


CM Windows Agent
Destination Location
Setup will install the CM Windows Agent in the following folder.
To install into a different folder, click Browse, and select another folder.
You can choose not to install the CM Windows Agent by clicking Cancel to exit Setup.
Destination Folder
C:\WINDOWS\CMAgent
Browse...
Lock Agent
Allow HTTP
Agent HTTP Port:
26542
< Back
Next >
Cancel

6. The installer proceeds with the installation. When the VCM Windows Agent has been successfully installed, click **Finish**.

7. Copy the following executable from your upgraded Collector machine to any location on your non-Collector Agent Proxy machine. The path to this file on the Collector machine is as follows, or is in the path relative to where you installed the software.

   ```
   C:\Program
   Files\VMware\VCM\AgentFiles\Products\VirtualizationProductInstall.exe
   ```

   Run the copied VirtualizationProductInstall.exe on your non-Collector Agent Proxy machine. This step begins the installation of VCM for Virtualization.

8. Proceed through the installation screens to install VCM for Virtualization.

9. The installer proceeds to install VCM for Virtualization. When VCM for Virtualization has installed successfully, click **Finish**. You can now begin collecting using your upgraded Agent Proxy.

NOTE If you have previously used this Agent Proxy to perform a collection from your upgraded Collector, the first collection may fail due to a password encryption issue. If so, try resetting the VM Host password at **Administration | Machines Manager | Additional Components | VCM for Virtualization | Licensed VM Hosts**. You may set the password for multiple hosts at the same time if desired.

All VCM-managed Windows machines will include the VCM Agent extension for VCM Provisioning, which is a separate installation.

For Agent Proxy machines, if the virtualization proxy and VCM Agent extensions for Provisioning are installed, you must run `ProvisioningProductInstall.exe` from the Collector.

Upgrading the vSphere Client VCM Plug-in

The vSphere Client VCM Plug-in integrates VMware vCenter Configuration Manager into the vSphere Client to provide VCM data and functionality within vCenter. After upgrading VCM, you must upgrade the Plug-in, which means vCenter users must un-register it and then re-register it.

Upgrading the Plug-In

To upgrade the vSphere Client VCM Plug-in, follow these steps:

1. Upgrade VCM.
2. Manually un-register the pre-VCM 5.3 version of the Plug-in, as described in Un-register the Previous Version of the Plug-in in Un-register the Previous Version of the Plug-in.
3. Register the new Plug-in by following the instructions in "Registering the vSphere Client VCM Plug-in" on page 143.

Un-register the Previous Version of the Plug-in

If you have already upgraded VMware vCenter Configuration Manager, you must manually un-register the previous version of the Plug-in before registering the VCM 5.3 Plug-in. Although the upgrade to VCM removes files for the previous Plug-in, and installs the new Plug-in files in new locations and with new names, it does not register the new Plug-in with the vSphere Client. To un-register the existing Plug-in, follow these steps.

1. Browse to the following link, where "`{vCenter machine name}`" is the name of your vCenter 4 Server instance:
   `https://{vCenter machine name}/mob/?moid=ExtensionManager`
2. In the **Methods** area, click the **UnregisterExtension** link.
3. Enter the following string value for **extensionKey**: **com.CM.VirtualCenterCompliancePlugIn**
4. Click **Invoke Method**.

Getting Started with VCM Components and Tools

4

This chapter covers global getting started procedures for VCM and all of its components and tools. After completing this chapter, you should proceed to the specific getting started chapters in this manual that apply to the components you have licensed and the VCM tools you plan to use. The remaining getting started chapters within this document build on this one. Therefore, you should have a solid understanding of the content within this chapter before proceeding to the remaining chapters.

This chapter contains the following sections:

- Understanding User Access
- Launching and Logging onto VCM
- Getting Familiar with the Portal
- Where to Go Next

Understanding User Access

After your installation is complete, the user who performed the installation is explicitly granted access and is placed in the roles of ADMIN and USER. This user is also placed into the Admin role. Hence, this user can immediately log in using the Admin role. The role of AD_Admin allows full administration access to AD objects only.

Other user accounts can then be added after the Admin user logs in by going to **Administration | User Manager | VCM Logins**. For instructions on how to add user accounts, see the online Help.

Whenever a user is either added to the Admin role in VCM, or granted access to the **Administration | User Manager** node, the user is placed in the fixed machine roles Security Administrators and Bulk Insert Administrators Groups. They are also added to the database roles public, ADMIN, and User on the VCM Database.

Users who will not have access to the **Administration | User Manager** node will be assigned to public. Depending on the functions granted to any particular user, more or fewer privileges may be needed in order for their role to function properly.

All VCM user accounts must have the following rights on the VCM Collector machine:

- Ability to log on locally to access IIS.
- Read access to the `System32` folder.
- Write access to the `CMFiles$\Exported_Reports` folder for exporting reports.
- If default permissions have been changed, read access to the `C:\Program Files\VMware\VCM\WebConsole` directory, along with all subdirectories and files.

Launching and Logging Onto VCM

If you have not already launched VCM after closing Installation Manager, follow the procedure detailed below to launch and log onto VCM.

IMPORTANT Before you launch VCM, you must either configure Internet Explorer Pop-up Blocker Settings to add your Collector to your list of allowed web sites, or disable Pop-up Blocker. Click **Internet Explorer** | **Tools** | **Popup Blocker Settings,** then add the path for your Collector in the allowable address field.

How to Launch VCM and Log On

1. If you are launching VCM on the Collector Machine, go to **Start** | **All Programs** | **VMware vCenter Configuration Manager** | **Web Console**. If you prefer to connect to VCM from another machine on your network, you may do so by pointing your browser to `http://<name_of_Collector_machine>/VCM`. For the specific browsers that are supported, refer to the *VCM Hardware and Software Requirements Guide*. The Logon screen appears.

vmware
VMware vCenter
Configuration Manager™
Enter your login information
Collector: DEVCOLL19
Domain Name: WP
User Name: bonnie.kern
User Role: Admin
Automatically log in using this role
Copyright © 1998-2010 VMware, Inc. All rights reserved.
This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
Login

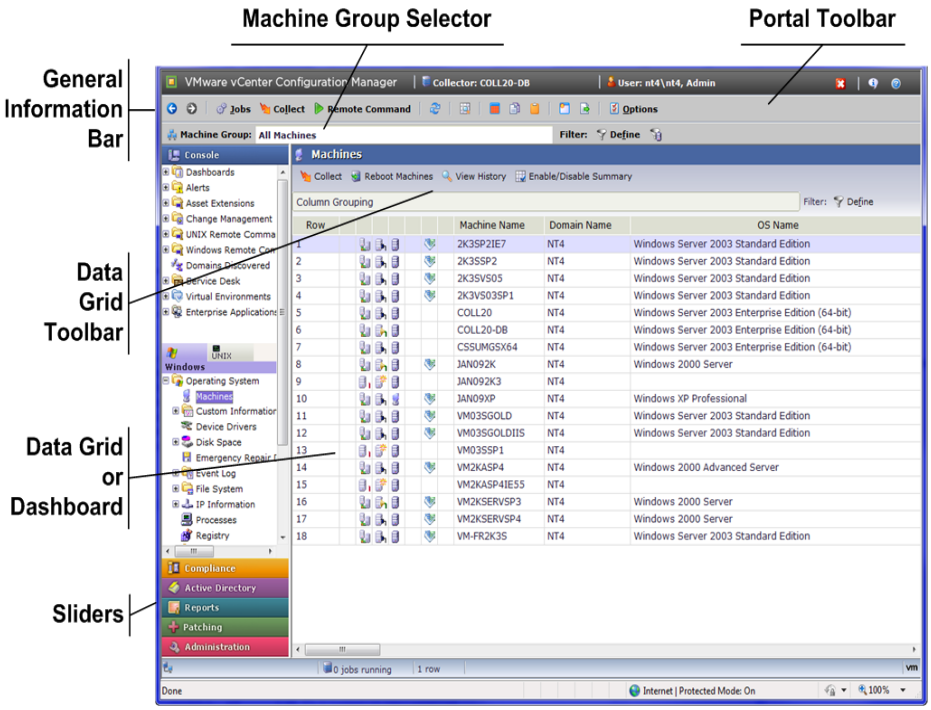
2. Depending on your browser security settings, you may have to supply your user network credentials.
3. (Optional) Select **Automatically log on using this role** to have VCM automatically log you on without prompting you for a role in the future.
4. Click **Log On**. The Portal appears.

In the future, your VCM user account may have multiple roles. At that time, if you have the Automatically log on using this role option checked, VCM will automatically log you on as the User Role displayed on the Logon screen. To change roles, you must use the Logoff button in the top right corner of the Console. This action will return you to the Logon screen so you can use the drop-down menu to select a different role.

Getting Familiar with the Portal

The VCM Portal uses a browser-based interface so it can be run from any Windows system running IE or with the IE tab plugin for Firefox, and having access to the machine on which VCM is installed. The Portal provides access to all VCM features for managing your enterprise.

As shown in the following diagram, there are several major controls and areas in the Portal. The following subsections describe the general information bar, global toolbar, and sliders in the Portal.



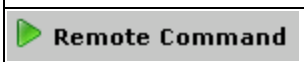
General Information Bar

The general information bar displays the VCM Collector's (active SQL Server) name, your VCM user name and active Role, and the following buttons:

- **Log Out:** Exits the Portal. The Portal closes, and the VCM Logon screen appears again.
- **About:** Displays information about how to contact VMware Customer Support. It also displays version information for VCM and all of its components. This information may be important when contacting VMware Customer Support.
- **Help:** Launches the online Help for the currently-active display.

Portal Toolbar

The global toolbar provides you with easily-accessible options to enhance control of your environment and data.

	The left and right arrow buttons navigate to the previous or next page in the data area.
	The Jobs button launches the Jobs Running status window. This button also provides access to the Collector status and allows you to stop/restart the Collector service.
	The Collect button launches a wizard allowing you to define and initiate data collections.
	The Remote Commands button allows you to invoke the Remote Commands wizard from the toolbar without having to access the node.
	The Refresh data grid view button refreshes the data grid view. Pressing F5 on the keyboard accomplishes this as well.
	The View row cells button displays a vertically scrolling view of a single row of data rather than the table-based data grid view in a separate window, and allows you to move between records.

	The Select all displayed data rows button selects all the rows in the data grid.
	The Copy button is used to copy information from the selected rows in the data grid to the clipboard.
	The Copy link to clipboard button is used to copy the link of the content on-screen to the clipboard.
	Click the View data grid in separate window button to display the data grid in a separate window.
	The Export displayed data button exports data to a CSV formatted file. This file is exported to \\<name_of_Collector_machine>\CMfiles$\Exported Reports.
	The Options button opens the User Options window. These settings pertain to the User who is logged on to VCM. All VCM Users will want to configure these to their individual preferences.

Sliders

The sliders on the left side of the Portal include the items listed and described in the following table. The individual items that you see in VCM will vary, depending on the components that you have licensed.

For detailed instructions regarding any of these features, refer to the online Help.

Select:	If you want to:
Console	■ View, export, or print enterprise-wide, summary information. ■ Review or acknowledge current alert notifications. ■ Manage both VCM discovered and non-VCM discovered hardware and software assets. ■ Review changes that occurred from one collection to the next. ■ Create, edit, or run remote commands on a VCM managed Windows or UNIX machine. ■ View information about VCM discovered domains. ■ Navigate and manage VCM-integrated service desk events. ■ Manage VCM-managed virtual machines. ■ View your Windows NT Domain and Active Directory related data. ■ View information for enterprise-level applications. ■ Review non-security related UNIX machine-specific information. ■ Review UNIX security data to ensure consistent security configurations across your enterprise.
Compliance	■ Create and manage Compliance rule groups and templates based on either AD objects* or machine group data.
Active Directory*	■ View, export, or print enterprise-wide, summary information for Active Directory objects. ■ Review alert notifications for the selected AD location. ■ Review Active Directory-related changes that occurred from one collection to the next. ■ View collected information about Active Directory objects such as Users, Groups, Contacts, Computers, Printers, Shares, and Organizational Units. ■ Review Active Directory site lists, including Site Links, Site Link Bridges, Subnets,

Select:	If you want to:
	Intersite Transports, Servers, Connections and Licensing. ■ View Active Directory Group Policy Container Settings. ■ View information about Active Directory Domains, DCs, and Trusts. ■ Track and display access control entries and security descriptor data on all collected objects. ■ View Active Directory Schema information.
Reports	■ Run "out-of-the-box" reports against your collected data. ■ Write your own SQL and SSRS reports using VCM's report wizard.
Patching(**)	■ Review a list of Microsoft bulletins available to VCM. ■ Create, run, or import VCM Patching templates to show which machines require the patches described in each bulletin. ■ Select machines to license, set options for assessment and deployment, or monitor VCM Patching jobs. ■ Deploy patches.
Administration***	■ Manage basic configuration options for VCM. ■ Establish filters to limit the data you collect from machines in your enterprise. ■ Manage your VCM licenses. ■ Organize and manage your enterprise using VCM. ■ Manage VCM Logins and Roles. ■ View the status of jobs that are currently running, scheduled to run, or completed. ■ Configure VCM to notify you of certain conditions in your enterprise.

* Available only when VCM for Active Directory (AD) is licensed. This slider is viewable based on your role.

** Available only when VCM Patching is licensed. This slider is viewable based on your role.

*** Visible only to users with Administrative rights to VCM as part of their VCM role.

Where to Go Next

You are now ready to proceed to Getting Started with VCM to start using VCM and all of its components and tools.

Once you have completed the steps in Getting Started with VCM, you must proceed to the next applicable chapter in this guide relevant to the components you have licensed in your installation. VMware has intentionally ordered the instructions in the remainder of this guide such that they build upon one another as you proceed through this guide; therefore, it is imperative that you proceed in order.

You can skip any chapters that do not pertain to your installation as you proceed through this guide in order.

NOTE If you choose to license another VCM component at a later date, you will be able to go back and configure it at that time.

Getting Started with VCM

5

Before you can begin using VCM to manage the machines in your enterprise, you must complete the following steps:

1. Discover, License, and Install Windows Machines.
2. Discover, License, and Install UNIX/Linux Machines.
3. Discover, License, and Install Mac OS X Machines.
4. Discover, License, and Collect Oracle Data from UNIX Machines.
5. Customize VCM for your Environment.
6. Set up and use VCM auditing.

Discover, License, and Install Windows Machines

The following steps must be performed before collecting data from Windows machines:

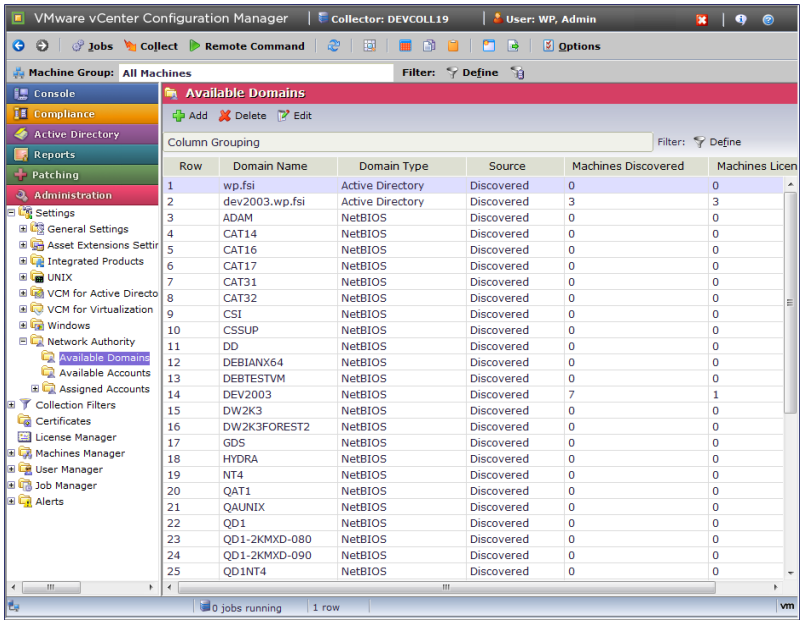
1. Verifying Available Domains
2. Checking the Network Authority
3. Assigning Network Authority Accounts
4. Discovering Windows machines.
5. Licensing Windows machines.
6. Installing the VCM Agent on your Windows machines.
7. Performing an initial Windows collection.
8. Exploring the Windows collection results.

These steps are explained in the following subsections.

Verifying Available Domains

The VCM Collector must gain access to each domain in order to interact with all enterprise Windows machines. During installation, VCM discovered all of the domains that the Network Authority Account you provided had access to.

To view a list of these discovered domains in VCM, navigate to **Administration** | **Settings** | **Network Authority** | **Available Domains**. VCM displays the available domains in the data grid.



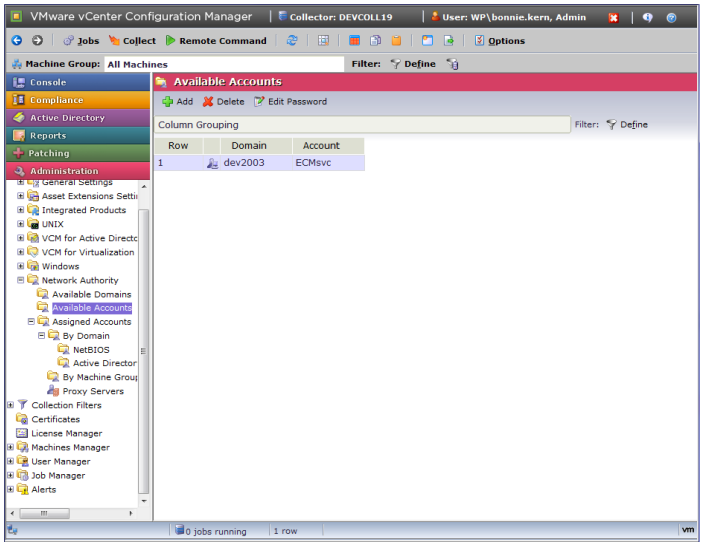
If the Windows machines that you want to manage belongs to a domain that is not shown in this list, then you must add that domain manually. Click **Add**, then follow the steps in the Add Domain wizard to manually add that domain. Once the domain is shown in the Available Domains list, you will be able to manage Windows machines in that domain.

Checking the Network Authority

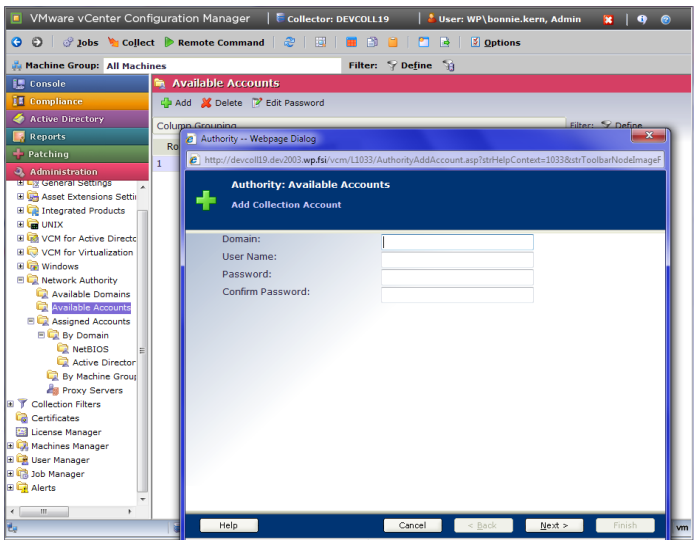
Your VCM Collector has to gain access to each domain to interact with the Windows machines in your enterprise. An account having Domain Administrator rights must be created for each domain that has Windows machines you want to manage. An initial account (your default Network Authority Account) was specified through VCM Installation Manager during installation; you may need to create others. Once an account has been created, it must be assigned to domains or machine groups (see Assign Network Authority Accounts).

The following procedure enables you to check for available accounts and add new ones if necessary.

1. Click **Administration** | **Settings** | **Network Authority** | **Available Accounts**.



2. If you need to add a new account, click **Add** and follow the prompts.



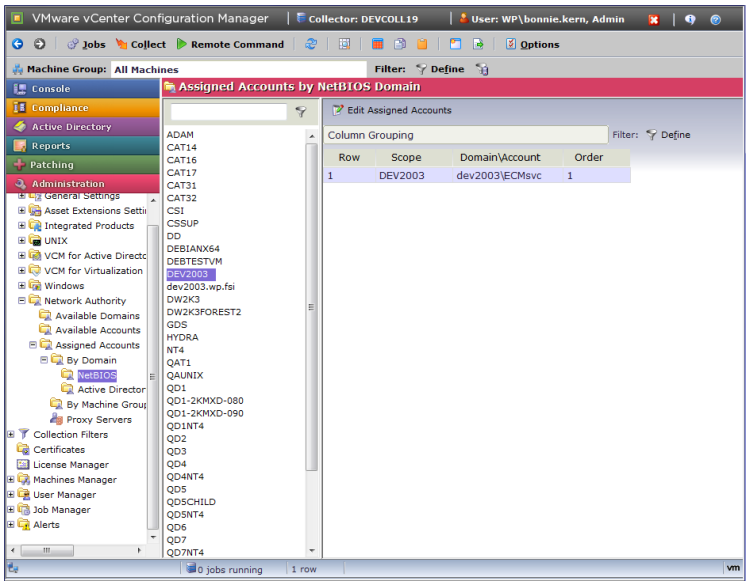
NOTE Repeat the Network Authority Available Accounts wizard, creating a specific account for each domain that has machines that you intend to manage through VCM.

Assigning Network Authority Accounts

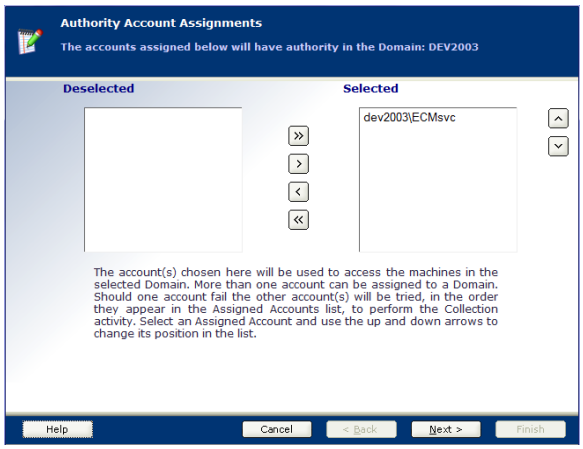
VCM offers considerable flexibility in assigning Network Authority Accounts to domains and machine groups. You can assign one account to all domains and machine groups, or assign a different account to each. You can even assign multiple accounts to each domain and machine group.

The following procedure illustrates how to assign Network Authority to accounts by NetBios domain. However, you can also assign Network Authority by Active Directory Domain, or even by Machine Group (**Administration | Settings | Network Authority | Assigned Accounts | By Machine Group**). For more information on these options, see the online Help.

1. Click **Administration | Settings | Network Authority | Assigned Accounts | By Domain** and then select **NetBios**.
2. Select a listed domain.



3. Click **Edit Assigned Accounts** and follow the prompts.


Authority Account Assignments
The accounts assigned below will have authority in the Domain: DEV2003
Deselected
Selected
dev2003\ECMsvc
The account(s) chosen here will be used to access the machines in the selected Domain. More than one account can be assigned to a Domain. Should one account fail the other account(s) will be tried, in the order they appear in the Assigned Accounts list, to perform the Collection activity. Select an Assigned Account and use the up and down arrows to change its position in the list.
Help
Cancel
< Back
Next >
Finish

Discovering Windows Machines

The discovery process identifies which machines can be accessed on your network. VCM uses one or more Discovery Rules to discover the machines that are present on your network and available to VCM. The Discovery Rules can be very general to discover many machines, or very precise to discover a particular subset of your machines.

Your initial discovery can take anywhere from one afternoon to a couple of days, depending on the size of your network. You may not have a 100% success rate with the first discovery process you run because some machines may not be available during that time (for example, laptops that are not currently on the network). It may, therefore, take a few days to coordinate and resolve scenarios in order for you to discover the machines in your enterprise.

NOTE It is not necessary to complete the discovery of every machine in your enterprise before you proceed with licensing machines. If you choose to move forward and license a subset of your machines, be sure to review these chapters when you discover additional machines at a later time.

All discovered Windows machines will be placed in the **Administration | Machines Manager | Available Windows Machines** list, and all discovered UNIX/Linux machines will be placed in the **Administration | Machines Manager | Available UNIX Machines** list.

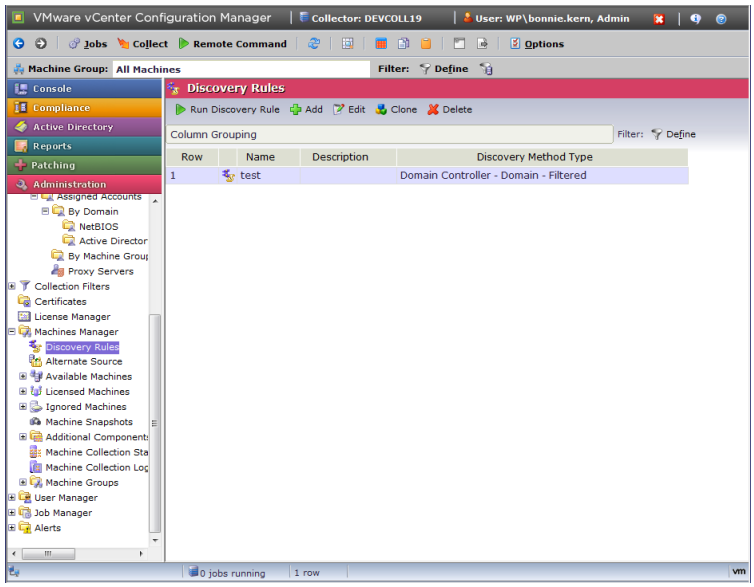
NOTE A Discovered Machines Import Tool (DMIT) is available from VMware Customer Support to assist you with the following process. This tool imports machines discovered by the Network Mapper (Nmap) into the configuration database. To use the tool, contact VMware Customer Support; otherwise, use the following process.

After the initial discovery, VMware recommends that you generally perform a discovery about once each week to keep the list of available machines current. You can schedule these future discoveries during your organization's off-hours, if you prefer.

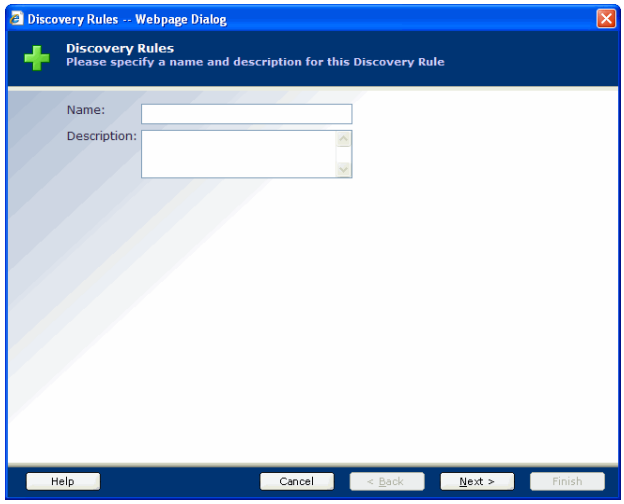
NOTE To schedule a VCM job for discovery, go to **Administration | Job Manager | Scheduled** and follow the Wizard. Refer to the online Help for more information.

Use the following procedure to discover machines.

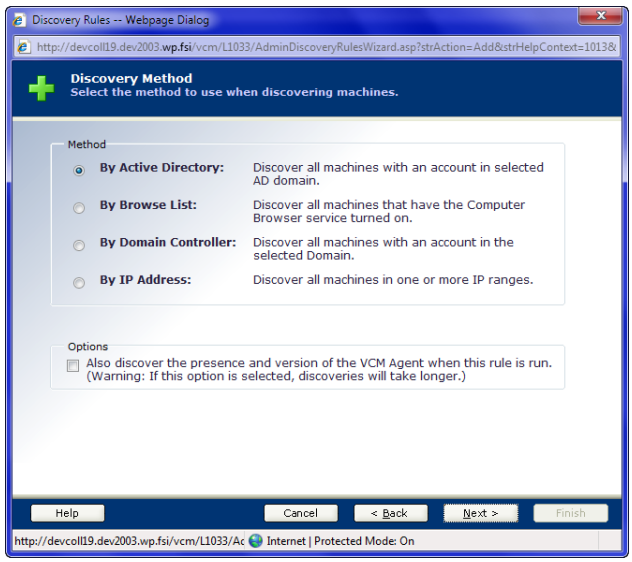
1. Click **Administration | Machines Manager | Discovery Rules**.



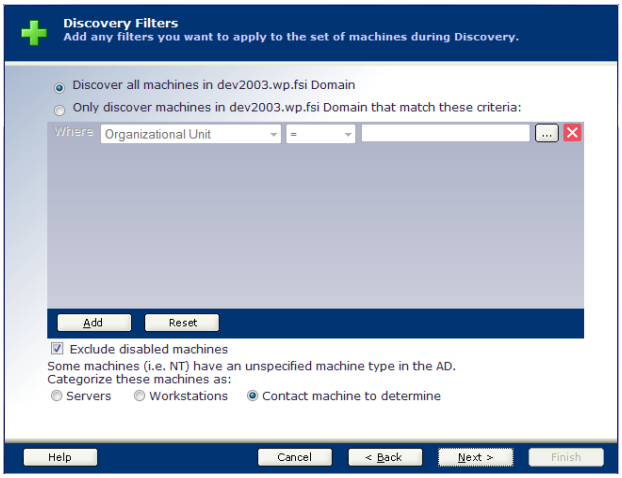
2. Click **Add** to create a Discovery Rule. The Discovery Rules wizard appears.



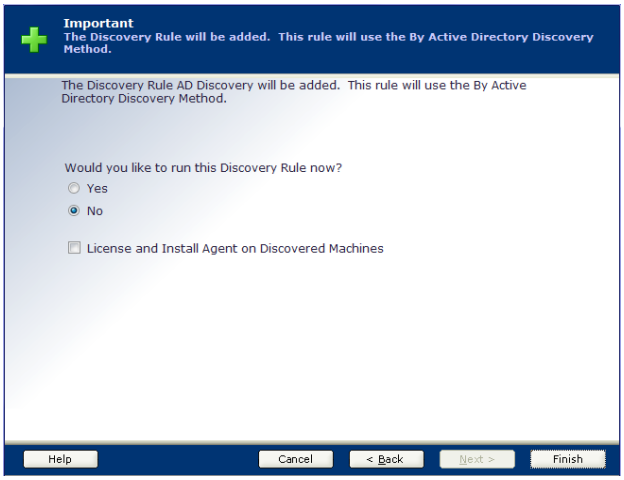
3. Type a **Name** and **Description** for this new Discovery Rule, then click **Next**. The **Discovery Method** page appears.


Discovery Rules -- Webpage Dialog
http://devcoll19.dev2003.wp.fsi/vcm/L1033/AdminDiscoveryRulesWizard.asp?strAction=Add&strHelpContext=1013&
Discovery Method
Select the method to use when discovering machines.
Method
By Active Directory:
Discover all machines with an account in selected AD domain.
By Browse List:
Discover all machines that have the Computer Browser service turned on.
By Domain Controller:
Discover all machines with an account in the selected Domain.
By IP Address:
Discover all machines in one or more IP ranges.
Options
Also discover the presence and version of the VCM Agent when this rule is run. (Warning: If this option is selected, discoveries will take longer.)
Help
Cancel
< Back
Next >
Finish
http://devcoll19.dev2003.wp.fsi/vcm/L1033/Ac
Internet | Protected Mode: On

4. If you have Active Directory in your environment, VMware recommends a discovery that is targeted for Active Directory. Select **By Active Directory**.
5. For an initial discovery, do not select **Also discover the presence and version of the VCM Agent when this rule is run**. Because the VCM Agent is not present on the machines yet, you cannot discover the Agent version.
6. Click **Next**. If you used By Active Directory, the **AD Domain** page appears.
7. Specify the **AD Domain**, accept the defaults, and then click **Next**. The **Discovery Filters** page appears.



8. Create the filter. For more specific filtering of machines for discovery and other advanced features, refer to the online Help. Click Next. The **Important** page appears.


Important
The Discovery Rule will be added. This rule will use the By Active Directory Discovery Method.
The Discovery Rule AD Discovery will be added. This rule will use the By Active Directory Discovery Method.
Would you like to run this Discovery Rule now?
Yes
No
License and Install Agent on Discovered Machines
Help
Cancel
< Back
Next >
Finish

9. Select **Yes** so that you can run the Discovery Rule immediately. Because you are discovering machines for the first time, you want to run the discovery now. Leave **License and Install Agent on Discovered Machines** unselected. If the box is checked, VCM will proceed with licensing and installing the Agent on each machine discovered, potentially exceeding your license count. For future scheduled discoveries, VMware suggests checking the box, but not for your initial discovery.
10. Click the **Jobs** button at the top of the Portal to verify that your discovery job has completed before proceeding to the next step. The Jobs Running window appears, listing your job name and summary information. If the job has completed, it will not appear here.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your running discovery job by going to **Administration | Job Manager | History | Other Jobs| Past 24 Hours**. Refer to the online Help for additional information regarding VCM Jobs.

Licensing Windows Machines

You are now ready to license the Windows machines you have discovered. In the following sections, you will license, install VCM Agents on, and collect data from your Windows machines. Later, we will guide you through these actions on your UNIX/Linux machines.

VCM requires that you specify the machines you want to manage. Remember, the number of licenses you have purchased may not match the number of machines that have been discovered and are visible in **Administration | Machines Manager | Available Machines | Available Windows Machines** or **Administration | Machines Manager | Available UNIX Machines**.

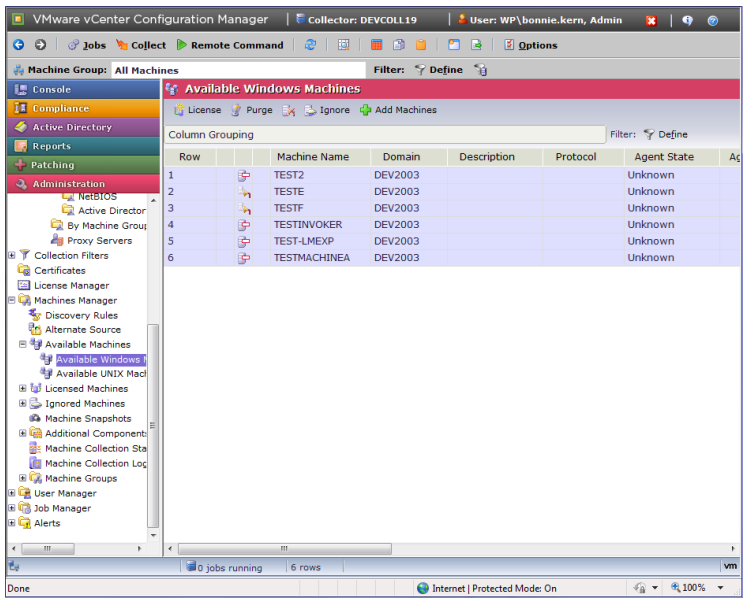
IMPORTANT If the machine type (that is, workstation or server) of a discovered Windows machine is indeterminate, then the machine cannot be licensed. The machine type is visible in the second column of the Available Machines Data Grid found at **Administration | Machines Manager | Available Machines | Available Windows Machines**. If you need assistance resolving the machine type for machines you plan to license, contact VMware Customer Support for guidance.

Use the following procedure to license your Windows machines.

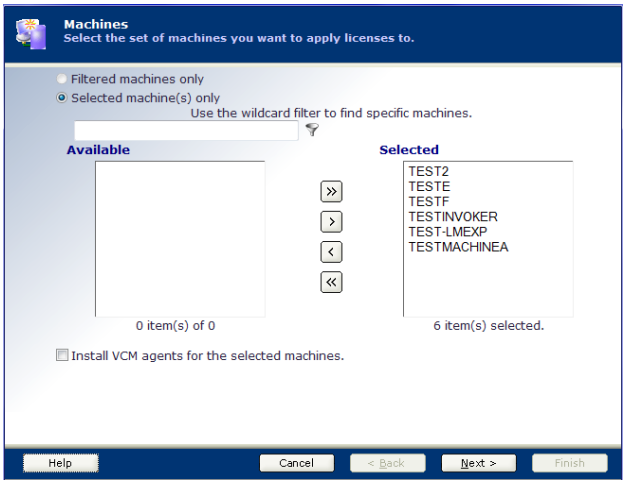
1. Select **Administration | Machines Manager | Available Machines | Available Windows Machines**.

   NOTE Remember, discovered machines with an indeterminate **Machine Type** will not be licensed if they are included in your selection.

2. Select the machine(s) you want to license. To select multiple machines, use **Shift-click** or **Ctrl-click**.



3. Click **License**. The Available Machines License dialog box appears.



4. Leave the **Install VCM Agents for the selected machines** box unchecked during your first pass at licensing machines. Once you have more experience licensing machines and deploying the VCM Windows Agent, you may choose to check this box when licensing. The machines that you selected appear in the Selected area. Click **Next** to view your Product License Details. The licensed machine count has increased by the number of machines that you have selected to license.
5. Click **Next**. VCM confirms that the licenses you requested will be applied to the selected machine(s).
6. Click **Finish**.

Installing the VCM Windows Agent on your Windows Machines

Before you can collect data from a machine, the VCM Windows Agent must be installed on your licensed Windows machine. You can install the VCM Windows Agent through VCM or manually. Both methods are described here.

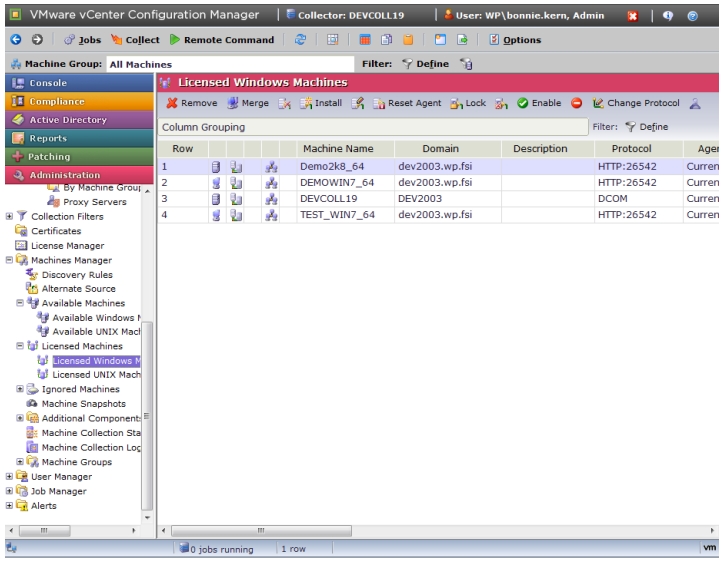
Machines that will be affected are those that are listed in the **Administration | Machines Manager | Licensed Machines | Licensed Windows Machines** view.

The following procedure describes how to install the VCM Windows Agent on your licensed Windows machines.

NOTE If you are installing the Agent on Windows 7, 2008, 2008 R2, or Vista, you may need to disable the UAC during installation. See"Disabling UAC for Agent Installation" on page 214 for information.

Use the following steps to install the VCM Windows Agent on your licensed Windows machines.

1. Navigate to **Administration | Machines Manager | Licensed Machines | Licensed Windows Machines**.
2. Select the Windows machine(s) on which you want to install the VCM Windows Agent. To select multiple machines, use **Shift-click** or **Ctrl-click**.



3. Click **Install** and follow the prompts.

NOTE To use advanced options such as HTTP communication for your agent, or to deploy the agent from an alternate source, refer to the online Help. To access the online Help at any time during the wizard, click the **Help** button in the lower left corner of the dialog box.

---

4. Verify that your agent installation job has completed. To check the status of an active job, click the **Jobs** button at the top of the Portal window to access the Jobs Summary.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your running discovery job by going to **Administration** | **Job Manager** | **History** | **Other Jobs** | **Past 24 Hours**. Refer to the online Help for details regarding VCM Jobs.

Manually Installing the VCM Windows Agent

You can manually install the VCM Windows Agent using either the EXE (.exe, executable) file or the MSI (.msi, Microsoft Installer) file that is supplied with VCM. Choose your install method based on the following:

- EXE files detect an existing software version and provide the option to uninstall the existing version. EXE files can also be used for unattended silent installations.
- MSI files are database files executed by the Windows MSIEXEC.EXE executable, which reads data in the MSI file and executes the installation. MSI files can be used for unattended, silent installations. The MSI installer will also uninstall an existing agent (non-msi), but it does not ask. If you run it again, you have the option of removal only. If you upgrade an MSI-installed agent with the new MSI, the old agent is uninstalled.

The VCM Enterprise Certificate, which is selected during the initial installation of VCM, is installed in the certificate store on the Agent machine during the Agent installation process if HTTP is selected. The Collector root certificate (Enterprise Certificate) is used to authenticate requests from a collector (using the Collector Certificate and its established trust to the Enterprise Certificate) on the Agent machine before a collection/change request is processed.

Using the .exe

To manually install the VCM Windows base Agent (CMAgentInstall.exe) on a target machine using the .exe file, follow these steps.

1. On your Collector, navigate to the Agent files directory at:
   `c:\Program Files\VMware\VCM\AgentFiles`
2. Locate the `CMAgentInstall.exe` file, and then install it from a network share or copy it to the target machine.
3. Navigate to the collector data directory at: `c:\Program Files\VMware\VCM\CollectorData`. Locate the Enterprise Certificate `.pem` file. This file must be accessible during the agent installation. The path used here is the default location. If your files are not in the default location, click **Administration | Settings | General Settings | Collector**. In the data grid, go to the **Root directory for all collector** files. The current path is displayed in the **Value** column.

   NOTE If the Enterprise Certificate has been distributed by a mechanism outside of the scope of VCM, such as a corporate Public Key Infrastructure (PKI), you may not need to include the Enterprise Certificate file.

4. In Windows Explorer, double-click the `CMAgentInstall.exe`. You will be asked for the certificate path and port.

   If you are performing a silent install, on the target machine run the `CMAgentInstall.exe` using the following parameters:

   ```
   CMAgentInstall.exe /s INSTALLPATH=%Systemroot%\CMAgent PORTNUMBER=26542
   CERTIFICATEFILE=<filename>
   ```

   NOTE The %Systemroot% environment variable specifies the directory where Windows is installed (typically \WINNT or \WINDOWS).

   Where:

   - **`CMAgentInstall.exe`** is the executable used to install the Agent.
   - **`/s`** indicates a silent install, which means that popups and menus do not appear. When running this command from the command line, VMware recommends using the /s option. When performing a silent install, if the VCM Windows Agent is found locked, the installation will fail. To unlock the Agent so that the installation will proceed, use the -UNLOCK option. When used, the Agent will remain unlocked when the installation completes. The syntax is:
     `CMAgentInstall.exe /s -UNLOCK INSTALLPATH=%Systemroot%\CMAgent PORTNUMBER=26542 CERTIFICATEFILE=<filename>`

     NOTE To re-lock your machine, submit a lock request from the VCM Collector.

   - **`INSTALLPATH`** is the location where the Agent will be installed.
   - **`PORTNUMBER`** is specified for HTTP Agents. If the PORT parameter is not present, the protocol will be DCOM. In this case, the communication socket listener service will not be installed and the certificate is not required.
   - **`CERTIFICATEFILE`** is the certificate that was generated or specified on the Collector during the Collector installation. The location of the certificate file will be in the path relative to where you installed the software on the Collector, and by default is `C:\Program Files\VMware\VCM\CollectorData\[certificate name].pem`. If you specify a PORTNUMBER, but do not want to use a certificate, you must use the parameter CERTIFICATEFILE=SKIP to allow an HTTP Agent without a valid CERTIFICATEFILE path.

NOTE **For Vista, Windows7, and Windows 2008 only:** If you set compatibility mode on any Agent executables to a prior version of Windows, the operating system may be reported incorrectly in VCM.

To Manually Uninstall the VCM Windows Agent

The VCM Windows Agent uninstall executable will be present only if the Agent was installed manually using CMAgentInstall.exe or CMAgentInstall.msi. To uninstall the VCM Windows Agent manually, execute the following command (this command assumes the default installation directory was selected):
`%SystemRoot%\CMAgent\Uninstall\Packages\CMAgentInstall\UnCMAgentInstall.exe`

Using the .msi

To manually install the VCM Windows base Agent (`CMAgent[Version].msi`) on a target machine using the .msi file, follow these steps:

1. On your Collector, navigate to the agent files directory. The location of the .msi will be in the path relative to where you installed the software on the Collector, and by default is `c:\Program Files\VMware\VCM\AgentFiles`.
2. Locate the `CMAgent[Version].msi` file. This file must be accessible by the target machine.
3. Navigate to the collector data directory at: `c:\Program Files\VMware\VCM\CollectorData`. Locate the VCM Enterprise Certificate `.pem` file, and then copy this file to the target machine in a secure manner.

   NOTE If your Collector is operating in a full Public Key Infrastructure (PKI), and the client can validate the Collector root certificate (Enterprise Certificate), the `.pem` file is not necessary.

4. On the target machine, double-click the .msi or run the .msi file using the command line syntax. Command line options and parameters are described below.

   ```
   msiexec /Option <Required Parameter> [Optional Parameter]
   ```

   For example:
   ```
   msiexec.exe /qn /i "[PathToFile]\CMAgent[Version].msi" [PORTNUMBER=<available port>] [INSTALLDIR="<new path>"]
   ```

When executing the Windows installer file with default options, any existing Window Agent is removed. The new VCM Windows Agent is then installed in the `%SystemRoot%\CMAgent` directory, and will use DCOM to communicate. The `%SystemRoot%` variable defaults to `C:\WinNT` or `C:\Windows`.

For HTTP installs, where `PORTNUMBER` is set, you must also specify an Enterprise Certificate. To do so, use this syntax: `CERTIFICATEFILE="x:\[mypath]\[mycert].pem"`. If you specify `PORTNUMBER`, you must also provide `CERTIFICATEFILE` with either `SKIP` or the path to a certificate file.

Command line options, showing required and optional parameters, include the following. These options are all parameters to msiexec.

- **`/qb`** - Runs the command in a basic user interface, displaying the progress and error messages.
- **`/qn`** - Runs the command in quiet mode; no user interaction is required.
- **`/i`** - Specifies the command as an installation.
- **`/x`** - Specifies the command as an uninstall process.

- **PORTNUMBER:** Installs the Windows Agent on the port number specified, using HTTP instead of DCOM. For HTTP installs, where PORTNUMBER is set, you must also specify a certificate file using the syntax: `CERTIFICATEFILE="x:\[mypath]\[mycert].pem"`. For example:
  `msiexec.exe /qn /i "C:\temp\CMAgent[VersionNumber].msi" PORTNUMBER=2666 CERTIFICATEFILE="x:\mypath\mycert.pem"`
- **INSTALLDIR:** Changes the default root directory specification (`%SystemRoot%\CMAgent`). For example:
  `msiexec.exe /qn /i "C:\temp\CMAgent[VersionNumber].msi" INSTALLDIR="C:\VCM"`
- **CERTIFICATEFILE:** Specifies the Enterprise Certificate. For example:
  `CERTIFICATEFILE="x:\[mypath]\[mycert].pem"` or `CERTIFICATEFILE="SKIP"`

For more information about the command line options and descriptions, click **Start** | **Run** | **msiexec** or visit http://www.microsoft.com.

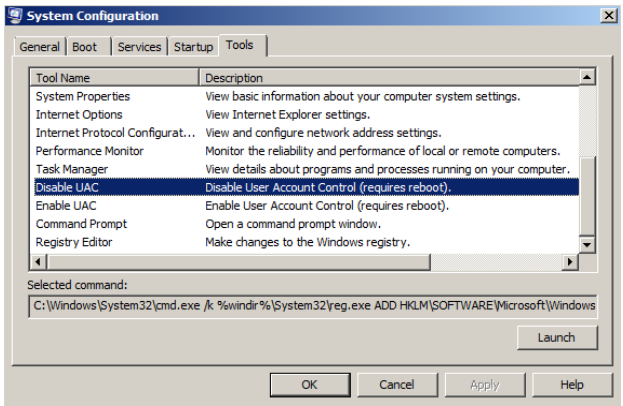
You must specify optional parameters using UPPERCASE letters, following the required "/i" parameter. Quotation marks are necessary only when a path includes spaces. For example, when one or more spaces exist in the source file location and the INSTALLDIR parameter. The optional parameters can be specified in any combination and order.

Disabling UAC for Agent Installation

The following steps are required only if you are installing the Agent on a Windows 2008 or Vista machine. When installing the Agent on Windows 2008 or Vista, you must disable the User Account Control (UAC), install the Agent, and then re-enable the UAC.

Disabling UAC on One Machine

1. On the target Windows 2008 machine, click **Start** | **Run**. The **Run** dialog box appears.
2. Type **msconfig** in the **Open** text box.
3. Click **OK**. The **System Configuration** dialog box appears. (This dialog box differs for Windows 2008 R2 machines.)



4. Click the **Tools** tab.
5. In the **Tool Name** list, select **Disable UAC**.
6. Click **Launch**. A **Command** window displays the running action. When the command is completed, close the window.
7. Close the **System Configuration** dialog box.

8. Restart the machine to apply the changes.
9. Install the Agent as specified in Licensing and Deploying the VCM Agent.
10. After installing the Agent on the target machine, re-enable UAC. To enable, perform the steps specified above. In Step 5, select **Enable UAC** in the **Tool Name** list.
11. Restart the machine to apply the changes.

Disabling UAC using Group Policy

Use the following procedure to disable the UAC on multiple machines. The instructions assume you have configured the Windows 2008 and Vista machines targeted for Agent install in a common Active Directory domain/OU.

1. On a Domain Controller, click **Start | Run**. The **Run** dialog box appears.
2. Type **mmc** in the **Open** text box.
3. Click **OK**. The **Console** window appears.
4. Select **Console Root**, and then click **File | Add/Remove Snap-in. The Add or Remove Snap-ins** dialog box appears.
5. In the **Available snap-ins** list, double-click **Group Policy Management Editor**. The **Select Group Policy Object** dialog box appears.
6. Click **Browse**. The **Browse for a Group Policy Object** dialog box appears.
7. On the **Domains/OUs** tab, select the domain/OU to which the target machines belong, and then click **OK**.
8. On the **Select Group Policy Object** dialog box, click **Finish**.
9. On the **Add or Remove Snap-Ins** dialog box, click **OK**.
10. The domain/OU policy is added to the Console Root in the left pane.
11. Expand the added domain/OU and browse to **Computer Configuration | Policies | Windows Settings| Security Settings | Local Policies | Security Options**.
12. In the right pane, locate the **User Access Control** policies. On each of the policies specified below, right-click and select **Properties**. Configure as follows:
    - **User Account Control: Behavior of the elevation prompt for administration in Admin Approval Mode:** Elevate without prompting.
    - **User Account Control: Detect application installations and prompt for elevation:** Disabled
    - **User Account Control: Run all administrators in Admin Approval Mode:** Disabled
13. Restart the machine to apply the changes.
14. Install the Agent as specified in the previous section, "Licensing and Deploying the VCM Agent".
15. After installing the Agent on the target machines, re-enable UAC. To enable, perform the steps specified above. In Step 5, change the policies to Enabled.
16. Restart the machine to apply the changes.

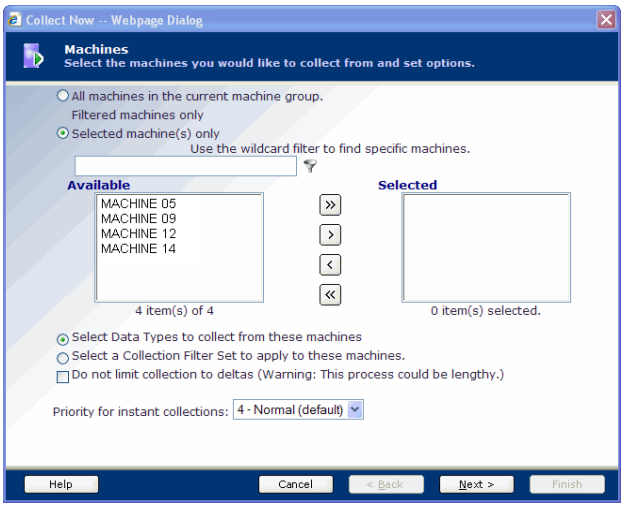
Performing an Initial Collection

You are now ready to collect data. VMware recommends using the default filter set, which collects a general view of the licensed Windows machines in your enterprise configuration, until you are ready to build specific filters and target your collections. The first time you use the default filter set for a collection, the VCM Agent will return all of the data (as specified by the filters in the default filter set) to be stored in the VCM database. Subsequent collections using the default filter set will return only a delta collection (meaning the differences between the data found on the target machine and what is already stored in the VCM database), unless you specify within the Collect Wizard to return the full collection. The delta collection feature makes subsequent collections run faster and more efficiently than the initial collection with that particular filter set.

IMPORTANT You can run Compliance Templates and perform reporting on data that has been collected and stored in VCM. Therefore, it is necessary to perform collections on a regular basis. This ensures that the data you are reporting on is current. When performing a full collection on your entire enterprise, you may want to run VCM overnight because the collection could potentially affect the performance of your machines. Once the initial collection completes, any future delta collections should be unnoticed by users. Be sure to perform collections on a routine basis to ensure accurate reporting.

---

1. Click **Collect**, located on the main Portal toolbar. The **Collection Type** page of the wizard appears.
2. Select **Machine Data**, and then click **OK**. The **Machines** page appears.

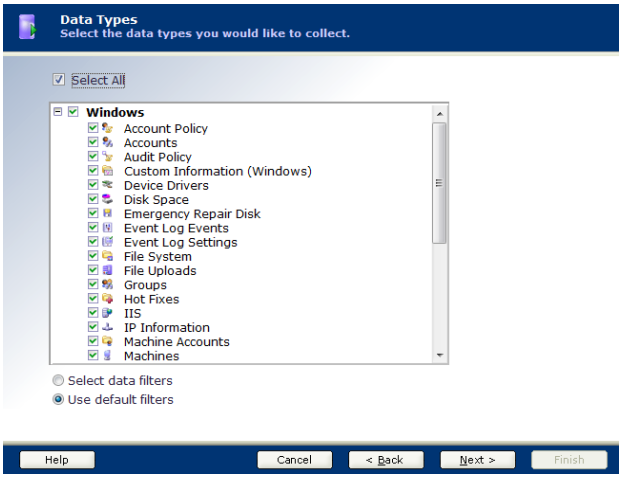

Collect Now -- Webpage Dialog
Machines
Select the machines you would like to collect from and set options.
All machines in the current machine group.
Filtered machines only
Selected machine(s) only
Use the wildcard filter to find specific machines.
Available
Selected
MACHINE 05
MACHINE 09
MACHINE 12
MACHINE 14
4 item(s) of 4
0 item(s) selected.
Select Data Types to collect from these machines
Select a Collection Filter Set to apply to these machines.
Do not limit collection to deltas (Warning: This process could be lengthy.)
Priority for instant collections:
4 - Normal (default)
Help
Cancel
< Back
Next >
Finish

3. Select the machine(s) from which you want to collect data. To select multiple machines, use Shift-click or Ctrl-click. Use the double arrow to move all visible machines to the selection window, 500 at a time. Leave the default options selected, then click **Next**.

   IMPORTANT To collect from machines running Windows XP SP2 or Vista using DCOM, you must either enable ICMP pings in the firewall settings, or disable ICMP pings in the Portal. Refer to the online Help for more information.

   ---

4. The Data Types dialog box appears. Check the **Select All** checkbox, then confirm that the **Use default filters** option button is also selected. Click **Next**.



5. For initial collections, there should be no conflicts with previously scheduled or running jobs containing the same data types. Click **Finish**.
6. Verify that your collection job has completed before proceeding to the next step. To do so, click the **Jobs** button at the top of the Portal window to access the **Jobs Summary**.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your collection job by going to **Administration** | **Job Manager** | **History** | **Instant Collections** | **Past 24 Hours**. Refer to the online Help for additional detail regarding Jobs.

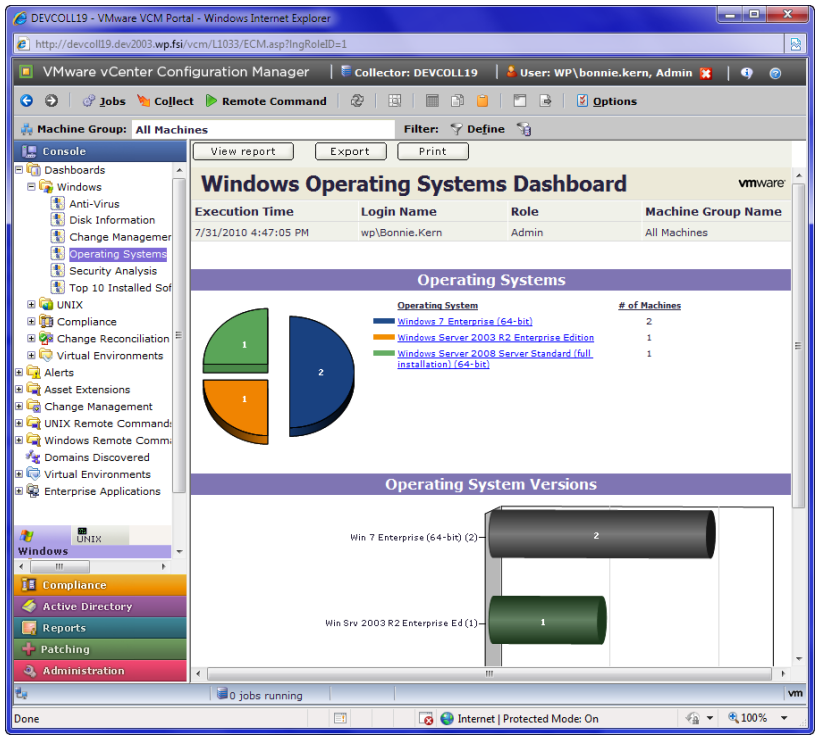
TIP Collecting certain Windows data types the first time results in a secondary SID lookup (looks up user accounts associated with a user ID) query back to the machine from which the data type was collected. To speed up initial collections that require a SID lookup, first collect the Accounts and the Groups data types from the Primary Domain Controller (PDC) of each domain. The PDCs have the necessary account information, and doing so automatically resolves the SIDs. The data types that cause the automatic additional query are:

- User Rights
- Registry Key Permissions
- Directory Permissions
- Share Permissions
- Disk Quota
- Event Log
- Services
- Processes

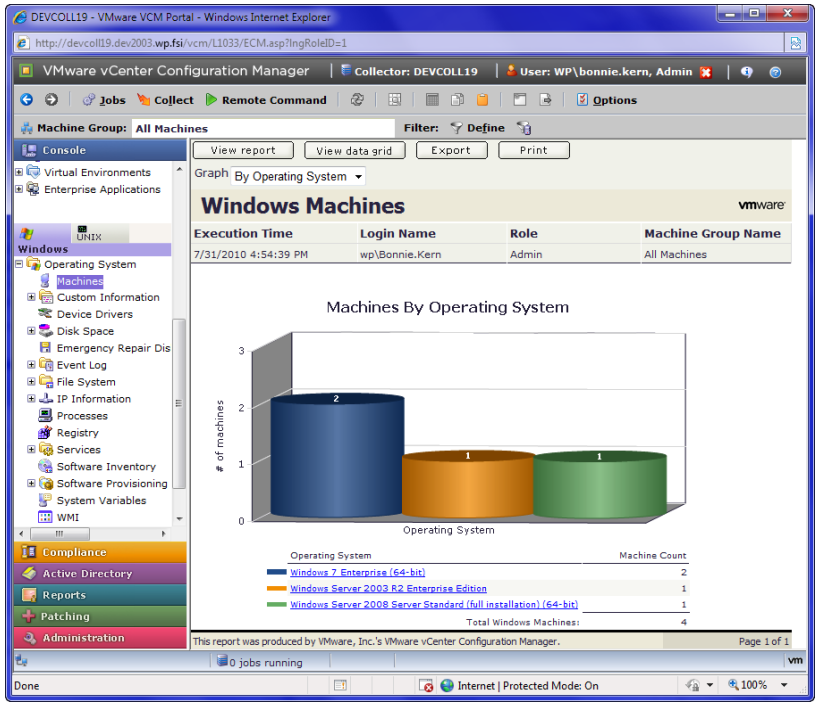
Exploring Windows Collection Results

Now that you have performed an initial Windows collection, you can explore that data in the VCM Portal. VCM presents summary information in graphical SSRS charts, for machines in the active machine group, which you can view, export, or print. The individual VCM Dashboards visible in the VCM Portal will vary, based upon which VCM components you have licensed. Each VCM Dashboard is run only when the node is selected against the current data available in the CMDB for machines in the active machine group. Therefore, Dashboard data is only current as of the time when it was collected. In addition, it may take time for the data to display based upon the volume or complexity of the data requested.

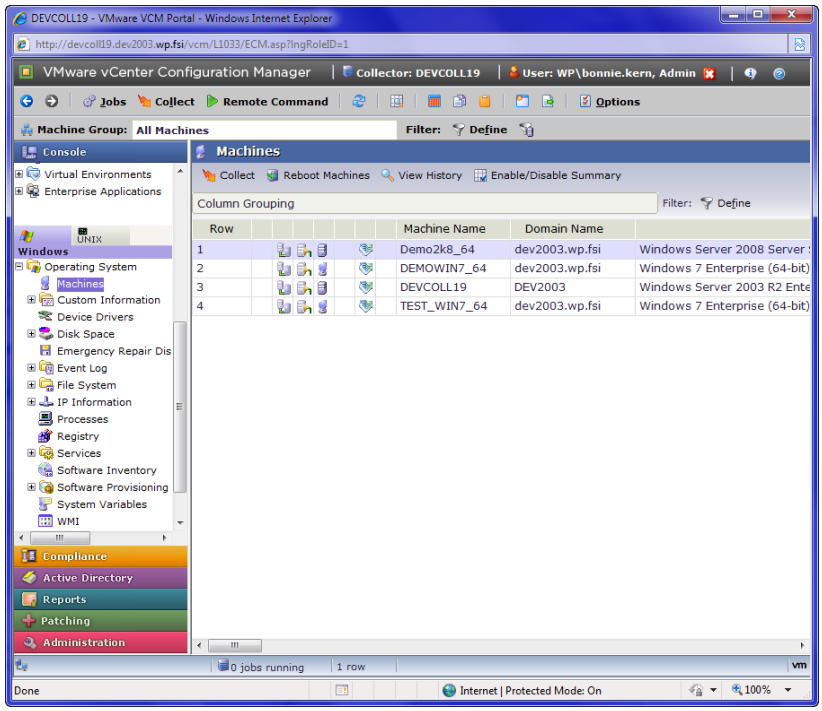
1. Begin by looking at the Windows Operating Systems Dashboard under **Console** | **Dashboards** | **Windows** | **Operating Systems**.



2. Note that several other Windows Dashboards are also available. Take time to familiarize yourself with the remainder of the Windows Dashboards. Windows Collection Results are also available to you in a more "raw" format by data class. This level of "reporting" is more relevant for day-to-day operations, troubleshooting, and analysis, and can be viewed in a Summary report or data grid format.
3. Now take a look at your Windows Operating System Information by clicking the **Windows** tab in the Console. Then, click **Operating System** | **Machines**.



4. When you select the node, you will see a Summary Report as displayed above of the data class that you selected. Click **View Data Grid** to go directly to the data grid, or click an area of the Summary Report to filter the data before the data grid is displayed.

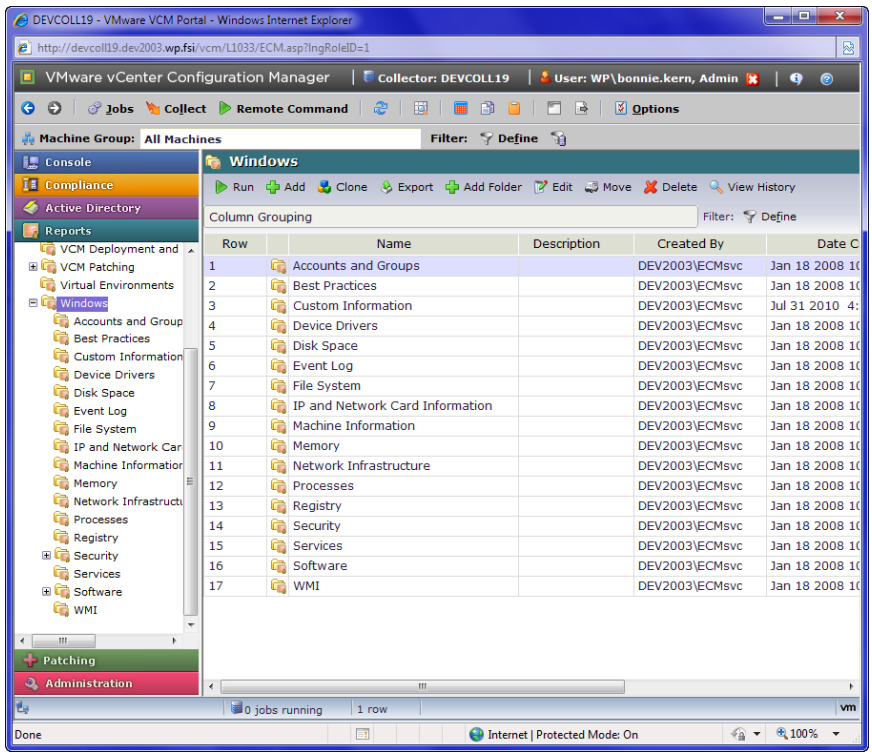


TIP The default view is the Summary Report; however, at any time you may switch the default view to go directly to the data grid by using the 'Enable/Disable Summary' feature on the data grid view. See About Data Grids in the online Help for more information on how to filter and sort your data and get full use of the data grid.

Several other categories (called "data classes") of information regarding your Windows Collection are available under the Windows tab, which is located in the Console. This is where the remainder of your collected Windows data is visible through the Portal.

An alternative way to view your collected Windows data is by running Reports or creating your own custom reports using the reporting wizard. To begin exploring VCM's Reporting functionality, go to the **Reports** slider, then click **Machine Group Reports | Windows**.

Like Dashboards, Reports are run against the current data available in the CMDB for machines in the active machine group, and therefore are only as current as the last collection. In addition, the report may require significant time to generate based upon the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.



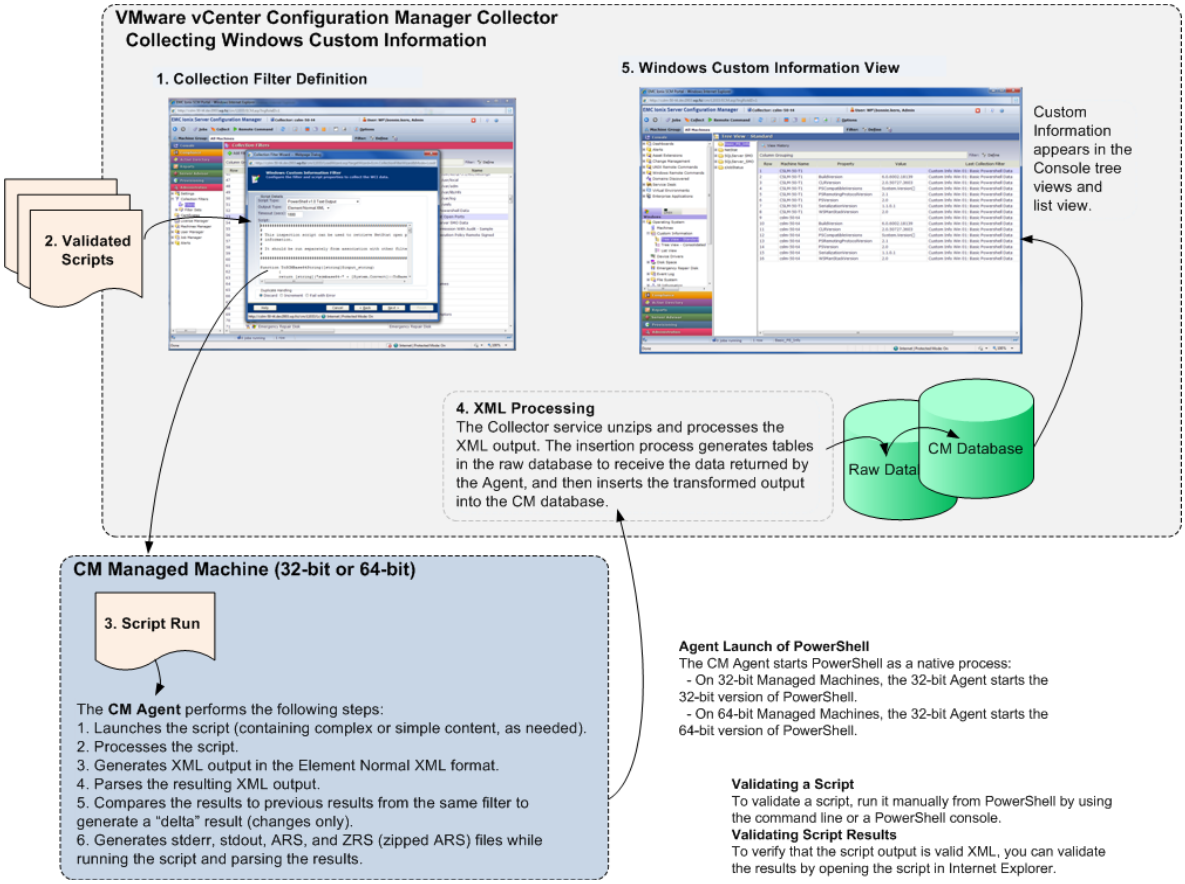
5. You may now begin to check Compliance for your collected data. To run a Compliance check, click the **Compliance** slider, then follow the steps as described in the online Help to create rule groups, rules, filters, and templates.

Getting Started Collecting Windows Custom Information

As a System Administrator, you can extend the data that VCM can collect by using a script, which will allow you to view, report on, alert on, detect change on, and run compliance against data not currently exposed by VCM. This extension allows you to view, report on, alert on, detect change on, and run compliance against custom data not currently exposed by VCM.

You can use the Windows Custom Information data type to perform user-defined, script-based collections from VCM-managed machines. To collect the custom data, you build a collection filter, which includes a script and other parameters relating to the execution of the script and the handling of its results. When this filter is used in a collection, the VCM agent will call a script engine to run the script, and will then parse the results so they can be returned to the VCM database and displayed in the VCM console. As of this release, VCM supports PowerShell scripting and XML output.

During the collection process, the VCM Agent launches PowerShell to execute the script, which in turn generates an XML result file. The Agent then parses the XML result into a format that can be checked for changes (deltas), and then those changes are returned to the Collector.


VMware vCenter Configuration Manager Collector
Collecting Windows Custom Information
1. Collection Filter Definition
5. Windows Custom Information View
Custom Information appears in the Console tree views and list view.
2. Validated Scripts
4. XML Processing
The Collector service unzips and processes the XML output. The insertion process generates tables in the raw database to receive the data returned by the Agent, and then inserts the transformed output into the CM database.
Raw Data
CM Database
CM Managed Machine (32-bit or 64-bit)
3. Script Run
The CM Agent performs the following steps:
1. Launches the script (containing complex or simple content, as needed).
2. Processes the script.
3. Generates XML output in the Element Normal XML format.
4. Parses the resulting XML output.
5. Compares the results to previous results from the same filter to generate a "delta" result (changes only).
6. Generates stderr, stdout, ARS, and ZRS (zipped ARS) files while running the script and parsing the results.
Agent Launch of PowerShell
The CM Agent starts PowerShell as a native process:
- On 32-bit Managed Machines, the 32-bit Agent starts the 32-bit version of PowerShell.
- On 64-bit Managed Machines, the 32-bit Agent starts the 64-bit version of PowerShell.
Validating a Script
To validate a script, run it manually from PowerShell by using the command line or a PowerShell console.
Validating Script Results
To verify that the script output is valid XML, you can validate the results by opening the script in Internet Explorer.

Prerequisites

Before collecting Windows Custom Information (WCI), you must ensure the following prerequisites are met.

- You must obtain or write a PowerShell script that will return data in a VCM-compatible element-normal XML format.
- The VCM agent (for VCM 5.3 or later) must be installed on each VCM-managed machine used to collect the Windows custom information. Older agents must first be upgraded.
- PowerShell must be installed on each VCM-managed machine. PowerShell is installed by default on Windows 2008 R2 and Windows 7 machines. For Windows XP, 2003, 2003 R2, 2008, and Vista machines, PowerShell must be installed separately. You cannot install PowerShell on Windows 2000 or NT4 machines. In cases where PowerShell is not installed on the target VCM-managed machine, the WCI collection will return a "Not Executed" success status. See Job Status Reporting for WCI.
- Windows Custom Information supports PowerShell version 2.0, and should work with later versions of PowerShell as well.
- After installing PowerShell on a VCM-managed machine, you must reboot the machine to ensure that collections will work properly.
- If the VCM Collector will be used as a client for WCI collections, ensure that PowerShell is installed on the Collector machine.
- VCM ships with default Administration settings for Agent Thread (default is set to below normal thread priority) and Agent Data Retention (default is 15-day change log). However, you can change these settings if you desire.
- Before file-based PowerShell scripts can be executed by the WCI collection filter on the VCM Collector and/or the VCM-managed machine, you change the execution policy on the VCM-managed machines. The PowerShell execution policy on the VCM machine must be set to **Remote Signed**, **All Signed**, or **Unrestricted**. If the policy is set to **All Signed**, the scripts must be signed, and the appropriate certificates distributed before collections can be run.

Procedure

To collect and view Windows Custom Information from VCM-managed machines, follow these steps.

1. Obtain PowerShell script(s) from VMware Professional Services or another source (or you can write your own). For more information about scripts, see Getting Started with PowerShell Scripts.
2. Select **Administration** | **Collection Filters** | **Filters**.
3. Click **Add Filter** to add a collection filter. The **Collection Filter Wizard** appears.
4. Enter a name for the filter, and then click **Next**. The Data Type page appears.
5. Select **Windows**, and then the **Custom Information (Win)** data type. Click **Next**. The **Windows Custom Information Filter** page appears.
6. Select your **Script Type**, which defaults to **PowerShell v1.0 Text Output**.
7. Select the **Output Type** of **Element Normal XML**.
8. Specify the **Timeout** in seconds. This setting specifies how long the Agent will allow a PowerShell script to run before attempting to end the process. The purpose of this setting is to prevent blocked or excessively long-running scripts from blocking other Agent requests.
9. In the **Script** area, paste the content of your user-defined PowerShell script, which contains statements specific to the data type you will be collecting. Depending on your script, parameters to be configured may exist near the top of the script.
10. VCM handles violations of any duplicate path attributes in the PowerShell scripts through the Duplicate Handling settings. In the **Duplicate Handling** area, select one of the following: **Discard**, **Increment**, or **Fail with Error**.

11. Click **Next** and then **Finish**.
12. Run a collection using your new collection filter.
13. Ensure the job completes.
14. View data in the Custom Information nodes (**Console | Windows | Operating System | Custom Information**).

When the Windows Custom Information data is available in the VCM database, you can generate reports and enforce compliance.

Change Detection in Windows Custom Information Data

Deltas in WCI are maintained on a per-filter basis at the client side, which means that if multiple filters return data under the same top-level element name (such as NetStat), each filter will have its own change detection.

In the following example, using multiple filters that collect the same open ports data and return it under the NetStat top-level element name, if a client machine has just started listening on port 80, each filter will report this new data as a newly created value the first time the filter "sees" this data. The best practice is to avoid this type of overlap of filters.

For example, two copies of the **File Permission With Audit** filter could be created in order to collect file permissions data from different parts of the file system, but they should not overlap. Having one filter get data from `C:\` and another filter get data from `C:\Windows` would be a good practice. However, having one filter get data from `C:\Windows` with audit information and another filter get data from `C:\Windows` without audit information would not be a good practice because both filters would generate "new file" and "deleted file" events each time a new file was added or removed.

- For an element such as NetStat, only one filter should be used.
- For an element such as NTFS file system (`NTFSDirectory`), multiple filters would likely be used. For example, one filter would be used to obtain the details under `C:\`, and another filter would be used for `C:\Windows\System`. Both would merge under the `NTFSDirectory` top-level element, but there should be no overlap; instead they would each collect separate parts of the file structure to avoid "extra" change reporting.

Purge for Windows Custom Information

As with other data types, purge for WCI will purge all data for a machine. This means that if a single WCI filter is collected with the "Do not limit to delta" option selected, all WCI data for that machine will be purged from the client's master file and from the VCM database, and it will be replaced with the resulting data from the single filter.

Job Status Reporting for WCI

Job status reporting for WCI is provided on a per script/filter level, and includes detailed reporting about exit codes and process standard error output. As each script/filter is executed, VCM captures detailed results information during the execution of the WCI collection filter scripts.

You can view the detailed information in the VCM user interface in the **Administration | Job Manager | History** node by selecting the executed job and then selecting **View Details** in the Job History Machine Detail pane of a collection job that includes WCI data.

The Job History Machine Detail view displays a single row for each WCI filter included in the collection job. These rows provide information about the execution of the WCI scripts and the parsing of the script results. In cases where the script cannot be executed because prerequisite components are not installed or available (such as PowerShell is not installed), the status for a row will be "Not Executed." This status does not result in a failure for the inspection because PowerShell (or other script engines) are optional components and may not even be installable on all VCM-supported OS versions.

If a WCI collection job encounters errors on a machine, detailed information about the failure will be reported. The failure could occur during the launch of PowerShell, during script execution, or during the interpretation of the script results. For example, an error could occur in the PowerShell launch process if PowerShell is not installed on the VCM-managed machine. However, since PowerShell is an optional component, such a failure does not roll up as an error to the job level, although the job details will show Not Executed to show such skipped steps. On the other hand, if a PowerShell script generates errors due to syntactical or typographical defects in the script itself, these errors will roll up to a "completed with errors…" status at the collection job level.

Running Reports

Several reports are included for reporting on Windows Custom Information, including:

- **Netstat Open Ports:** Reports port and protocol information from the `netstat -A` command.
- **SQL SMO Database:** Reports database details collected.
- **SQL SMO Instance:** Reports basic information about SQL Server instances collected.

These reports are in **Reports** | **Machine Group Reports** | **Windows** | **Custom Information**.

Getting Started with PowerShell Scripts

The Windows Custom Information data type (WCI) uses extensions to the VCM Windows agent to allow the agent to invoke scripts that are passed down as part of a collection filter's parameters, and then parse the results. As a result, these extensions are very flexible in that they use filter parameters to detail the command line to invoke the scripting engine, and a COM class name to specify the parser the Agent will need in order to parse the script output. This allows the eventual extension of the system to support multiple different scripting engines/languages and multiple options for output format.

For this version of WCI, the base requirement supports PowerShell for the scripting engine and a specific XML format, named Element Normal XML, as the output.

This topic describes:

- Executing PowerShell Scripts
- Developing Custom Collection Scripts
- Example of Developing a Custom PowerShell Script for Use with the WCI Data Type
- Troubleshooting Custom PowerShell Filter Scripts

Executing PowerShell Scripts

PowerShell contains built-in policies, which limit its use as an attack vector. The primary policy is for script execution. By default the script execution policy is set to Restricted, which means that PowerShell can only be used interactively or for executing commands directly from the command line. The additional policy settings are as follows:

- **AllSigned:** Any PowerShell script (.ps1 is the typical extension) must be signed by a verifiable certificate (from the SPC certificate store)
- **RemoteSigned:** Any PowerShell script that is downloaded from the Internet (by a supporting browser such as Internet Explorer) must be signed. Script files that are created locally, or scripts that are downloaded by a means that does not support flagging of the file source, do not need to be signed.
- **Unrestricted:** All PowerShell script files will be executed regardless of whether they are signed.

In addition, PowerShell 2.0 adds the capability to set different script signing policies at the machine, user, and process (single execution of powershell.exe) scopes.

WCI uses Script Type information in the collection filter definition to indicate how PowerShell should be executed and how the script should be passed to it. The primary ways a WCI script may be passed to PowerShell is either in-line or through a script file

- **In-line:** Requires a collection script that can be represented as a single line of PowerShell code. In-line scripts can be run regardless of the execution policy; because an in-line script is run on the PowerShell command line rather than from a file, the execution policy does not apply. The default WCI filter uses an in-line script to collect basic information about the PowerShell version, .NET version, and execution policy settings of a system.
- **Script file:** Requires that the execution policy be set to Remote Signed at the most restrictive, since the script is being run from a file locally on the client system. Because of its additional ability to have execution policy set at the process level, PowerShell 2.0 is the base requirement for WCI in VCM. The default script type command line used for script based filters in WCI includes options to set the process-level execution policy to Remote Signed. This allows WCI to execute collection scripts against systems whose machine and user level signing policies may be anything, without having to change the setting. Out-of-the-box VCM WCI non-in-line collection filters will fail if executed against PowerShell 1.0 client systems.

VMware recommends that you upgrade from PowerShell 1.0 to PowerShell 2.0, which introduced a number of useful functions. PowerShell 2.0 is also supported on all platforms that support PowerShell 1.0.

It is possible to execute WCI PowerShell collection scripts against PowerShell 1.0 systems as well, although it has not been tested, and is not officially supported. In-line WCI filters that do not employ PowerShell 2.0 commands should work directly. For script file based filters to work, you must create them with the PowerShell v1.0 Text Output script type, and the system must already have its execution policy set to Remote Signed, at the most restrictive, with un-signed scripts, or to All Signed with signed scripts (see below). This setting can be accomplished by the Group Policy Object (GPO), through the use of a VCM Remote Command, or by using a registry change action or enforceable compliance to set the policy directly. For example:

```
HKLM\Software\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
"ExecutionPolicy"="RemoteSigned"
```

For additional information about Windows PowerShell and signing scripts, see:

- **Scripting with Windows PowerShell:** http://technet.microsoft.com/en-us/scriptcenter/dd742419.aspx
- **Windows PowerShell Owner's Manual:** http://technet.microsoft.com/en-us/library/ee176949.aspx
- **Signing Windows PowerShell Scripts:** http://technet.microsoft.com/en-us/magazine/2008.04.powershell.aspx
- **Execution Policies:** http://technet.microsoft.com/en-us/library/dd347641.aspx
- **Registry value that controls execution policy:** http://msdn.microsoft.com/en-us/library/bb648598(VS.85).aspx

Developing Custom Collection Scripts

Development of custom collection scripts requires planning the data structure. WCI internally stores data hierarchically, as displayed in the Tree View - Standard node. The collection script is required to provide all of the structure that can be seen in any branch under this node.

The root element in the XML result data set will become a top level (root) element in the WCI data type node. Child elements will appear in the same locations in the VCM user interface as the locations they populate in the XML document that is returned by the script.

When developing custom collection scripts, follow these guidelines:

- XML element names must be unique at their level (for example, two "Child1" nodes can exist, as long as they are not siblings).
- Attributes must be unique at their level.
- Element and attribute names used must be valid XML when returned by the script. If data is to be returned as an element or an attribute name that is not valid for XML, the name can be encoded using the [`ToCMBase64String`] function. The inserter will recognize names encoded with this function and will decode them during the raw insert process. The inserter is a Collector job that is executed during each collection. It is responsible for parsing the Agent results files and putting the data into a new raw database table. The raw data is then transformed into the data that appears in the nodes in the user interface.

```
function ToCMBase64String([string]$input_string)
{
return [string]("cmbase64-" +
[Sys-
tem.Co-
nvert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes($input_
string))).replace("=","-")
}
```

- If a script has configurable parameters, they should be described in a comment block near the top of the script, along with configurable entries of the parameters near the top of the script, so that a user who is cloning a WCI collection filter can easily see and set the parameters in the **Edit Filter** wizard (**in Administration | Collection Filters | Filters**).
- Declaration of variables, and any other tasks in a script that produce output that is not part of the XML result set, should be redirected to out-null, such as:

```
[reflection.assembly]::LoadWithPartialName("Microsoft.SqlServer.Smo") | out-
null
```

- The default WCI filter returns PowerShell version information from VCM-managed machines.

See also the example below of developing a custom PowerShell script for use with the WCI data type.

Example of Developing a Custom PowerShell Script for Use with the WCI Data Type

In this example, the objective is to collect scheduled tasks information from Windows clients. On newer systems, Windows conveniently provides the `schtasks.exe` utility to report on scheduled tasks created either through the Task Scheduler user interface or through use of the `AT` command.

- Running `schtasks` by itself returns only basic data about tasks.
- Adding the `/query /v` switches provides additional information, but the formatting is difficult for automated processing.
- The `schtasks /query /?` command provides additional possibilities.
- The option set of `schtasks /query /v /fo:csv` is selected as the source for the data for the collection script. These options give full details for all tasks in a comma-separated value result set.

PowerShell makes working with tabular result sets from commands easy. A first step for this script is to run a command similar to:

```
$schtasks = schtasks /query /v /fo:csv
```

Since the data returned from `schtasks` includes multiple rows, PowerShell makes the `$schtasks` variable into an array. As such, `$schtasks[0]` represents the first row returned from the command. Viewing the result set by looking at `$schtasks[n]` shows that that the first line, `$schtasks[0]`, is blank; `$schtasks[1]` contains column names, and `$schtasks[2]` is the first row of task data. The goal, then, is to parse this data into a structure compatible with VCM's XML format for return to the Collector.

The Scheduled Tasks script uses the split method of PowerShell strings to separate the columns of the `$schtasks` rows into separate values in arrays. The column names row provides the names to use for attributes, and the corresponding data from the scheduled task rows provide the values to use for these attributes.

Once parsed, the XML returned by the script should look something like:

```
<schtasks>
     <taskname1>
          <attribute1>Value1</attribute1>
          <attribute2>Value2</attribute2>
          …
     </taskname1>
     <taskname2>
          <attribute1>Value1</attribute1>
          <attribute2>Value2</attribute2>
          …
     </taskname2>
          …
</schtasks>
```

The `<schtasks>` top-level name is an arbitrary name picked to distinguish the results of this script from others. A couple of additional challenges must also be overcome with this data, related to column names returned by the `schtasks` command, and the fact that the `schtasks` command does not include any unique and repeatable identifier for specific task entries. Details about these challenges are described next.

The first challenge can be seen by looking at the column names returned by the `schtasks` command. Even the basic `schtasks` command (no options) has a column name of Next Run Time. Since this column name includes spaces, it cannot be used as-is as an attribute name in an XML document. Other column names returned by the more verbose execution of `schtasks` have similar problems. To preserve these column names in the form that they are returned from the `schtasks` command, but still allow for XML handling, the names are encoded with the `ToCMBase64String` function:

```
function ToCMBase64String([string]$input_string)
     {
     return [string]("cmbase64-" +
     [Sys-
     tem.Co-
     nvert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes($input_
     string))).replace("=","-")
     }
```

This function uses Unicode base64 encoding, along with some character substitution (a dash instead of an equal sign) to create an XML-legal form of any element or attribute name. The string is prefixed with `cmbase64-` to indicate to the VCM inserter that the data will need to be decoded prior to loading it into the VCM database. The end result is that rather than containing invalid data like this:

```
<Next Run Time>
 12:32:00, 5/26/2010
</Next Run Time>
```

The XML will contain this:

```
<cmbase64-TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
12:32:00, 5/26/2010
</cmbase64-TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
```

The second problem is that the `<schtasks>` command does not include any unique and repeatable identifier for specific task entries. For example, many test systems observed had more than one task with the name: `GoogleUpdateTaskMachineCore`. Unique element names are a requirement for valid VCM XML, and repeatable identifiers are desirable to prevent false indications of changes at the VCM Collector. For example, if the script was to arbitrarily label rows as Task1, Task2, …, and Task1 was deleted, Task2 would then become Task1, and VCM would show a lot of changed details for Task1 (command line changed, next run time changed, etc), when in fact, that task had not changed at all – it had only changed places in the sequence.

One way to handle creation of unique and repeatable names for elements is to create a name based on a hash of the data contained in the row. That is useful for data that has no name-type attribute at all. In this case, however, there is a task name, but it is not guaranteed to be unique. Since the task name is user-friendly and useful, it is desirable to try to preserve and use it through the collection script. To preserve it, the task name is used as the element name for task rows, but the “increment” option is selected for duplicate handling when creating a collection filter based on this script. This action allows the collection process to add an incremental entry to a list of multiple entries with the same task name: the first example of `GoogleUpdateTaskMachineCore`, while the second example will be relabeled as `GoogleUpdateTaskMachineCore_1`.

It is still possible that reordering the list among tasks that have the same name, will cause "extra" changes to be reported, but regardless of these changes, it is reasonable to have VCM display the friendly task names in the user interface. Because task names also can contain characters that would not be valid for XML element names, the task names, as with the column names, are encoded using the `ToCMBase64String` function.

Troubleshooting Custom PowerShell Filter Scripts

You can interactively test a custom PowerShell script using the following procedures.

Procedure

Verify the script runs correctly within a PowerShell shell.

1. Start PowerShell from the command line on a VCM-managed machine.
2. Paste the inspection script into the PowerShell shell window.
3. Depending on the last character, it may require one extra hit of the Enter key to start the script
4. The script should run to completion without throwing any errors (red text in the command line based powershell.exe environment).
5. Once completed, the script should return a set of XML, without any formatting white space (no CR LF at the end of elements, nodes, or attributes).
6. When this test is successful, run the script from a file.

Procedure

After you have verified the script runs correctly within PowerShell, run the script from a file:

1. Save the script to a .ps1 file.
2. From a command line run the script directly:
   - For PowerShell 2.0, execute: `PowerShell –command set-executionpolicy RemoteSigned –scope Process ; scriptname.ps1 > resultfile.xml`
   - For PowerShell 1.0 (with the execution policy already set to Remote Signed or less restrictive), execute: `PowerShell –file scriptname.ps1 > resultfile.xml`

   When the script is complete, the XML result file should be created.
3. Verify that the XML file in question can be opened in Internet Explorer (you may have to allow blocked content in order to see the entire file). If the XML file cannot be parsed by Internet Explorer, the formatting errors in the XML from the script will need to be corrected before the script can be used as a collection filter script. Visual Studio can be a useful tool for finding formatting errors in larger XML files.

For details the job status reporting for WCI, see Getting Started Collecting Windows Custom Information.

Discover, License, and Install UNIX/Linux Machines

The following steps must be performed before collecting data from UNIX/Linux machines:

1. Add UNIX/Linux machines.
2. License your UNIX/Linux machines.
3. Install the VCM Agent on your UNIX/Linux machines.
4. Perform an initial UNIX/Linux collection.
5. Explore the UNIX/Linux collection results.

These steps are explained in the following subsections.

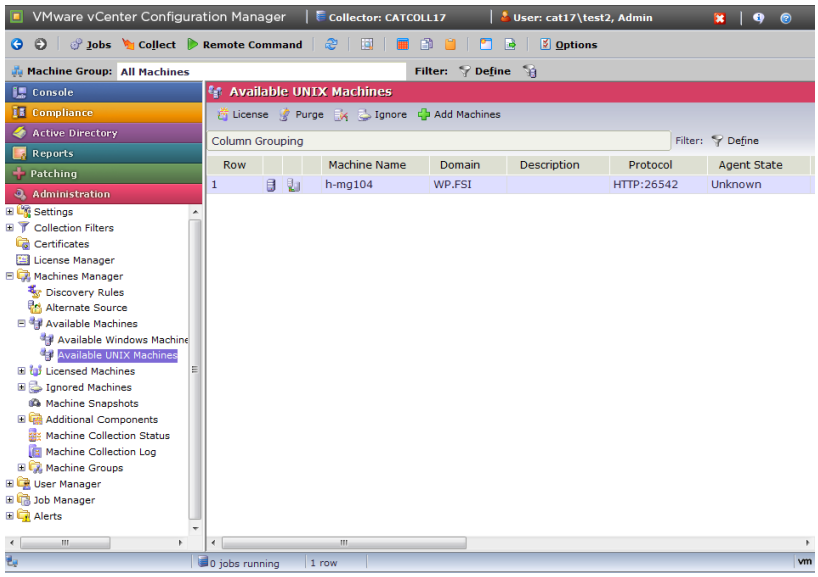
Adding UNIX/Linux Machines

Before you can collect data from your UNIX/Linux machines, they must be displayed in the Available UNIX Machines list located in the Portal under **Administration | Machines Manager | Available Machines**.

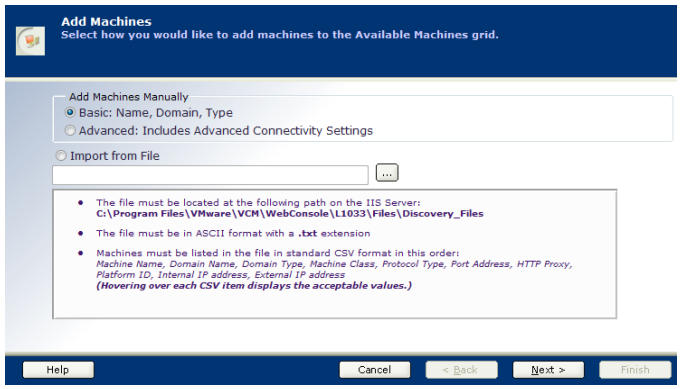
NOTE A Discovered Machines Import Tool (DMIT) is available from VMware Customer Support to assist you with the following process. This tool imports machines discovered by the Network Mapper (Nmap) into the configuration database. To use the tool, contact VMware Customer Support; otherwise, use the following process.

---

1. Click **Administration | Machines Manager | Available Machines | Available UNIX Machines**.



2. Click **Add Machines**. The **Add Machines** page appears.


Add Machines
Select how you would like to add machines to the Available Machines grid.
Add Machines Manually
Basic: Name, Domain, Type
Advanced: Includes Advanced Connectivity Settings
Import from File
The file must be located at the following path on the IIS Server:
C:\Program Files\VMware\VCM\WebConsole\L1033\Files\Discovery_Files
The file must be in ASCII format with a .txt extension
Machines must be listed in the file in standard CSV format in this order:
Machine Name, Domain Name, Domain Type, Machine Class, Protocol Type, Port Address, HTTP Proxy, Platform ID, Internal IP address, External IP address
(Hovering over each CSV item displays the acceptable values.)
Help
Cancel
< Back
Next >
Finish

3. Select **Basic**, and then click **Next**. The **Manually Add Machines - Basic** page appears.

NOTE When you expand your UNIX/Linux collections to a broader set of machines, you may want to use other methods to add your UNIX/Linux machines. Refer to the online Help for the advanced features such as importing from a file or using IP Discovery.

4. Enter the **Machine** and the **Domain**, and then select **DNS** for **Type**. For **Machine Type**, select the appropriate operating system. Modify the port number if you are not using the default.

NOTE The port number specified must be the same number used when the Agent is installed on the managed UNIX/Linux machine.

5. Click **Add** to add the entry to the list.
6. Repeat for any other machines.
7. Click **Next** and accept the changes.

NOTE If your Collector cannot resolve a host name with a DNS Server, be sure to use an IP address in place of a Machine name for your machines as you enter them.

Licensing UNIX/Linux Machines

When the UNIX/Linux machines are displayed in your Available UNIX Machines list, you may begin licensing these machines.

Upgrading Red Hat Workstations

In previous versions of VCM, Red Hat machines, either workstations or servers, were licensed as Red Hat servers. Beginning with version 5.2.0, Red Hat machines were licensed as either workstations or servers. When you upgrade to 5.2.0 or later, the workstations, previously managed with a server licenses, will be unmanaged in VCM. The unmanaged Red Hat workstations should be listed in the Available UNIX Machines list. To manage the machines in VCM, go to Administration | Machines Manager | Available Machines | Available UNIX Machines and re-license the machines using Linux/Mac Workstation licenses.

If you are unable to identify your now unmanaged Red Hat machines, contact VMware Customer Support.

Use the following procedure to license your UNIX/Linux machines.

1. Click **Administration | Machines Manager | Available Machines | Available UNIX Machines**.

NOTE Remember, discovered machines with an indeterminate **Machine Type** will not be licensed if they are included in your selection.

2. Select the machine(s) you want to license. To select multiple machines, use **Shift-click** or **Ctrl-click**.
3. Click **License**. The **Machines** page appears.
4. The machines that you specified appear in the **Selected** area. Add or remove machines from the list as needed.

5. Click **Next**. The **Product License Details** page appears.
6. The licensed machine count has increased by the number of machines that you have selected to license.
7. Click **Next**. The **Important** page appears.
8. Review the information.
9. Click **Finish**.

Installing the Agent on UNIX/Linux Machines

Before collecting data from your UNIX/Linux machines, you must install the VCM Agent on each licensed UNIX/Linux machine. For information about upgrading existing Agents, see the online Help.

IMPORTANT The Collector should be installed before the Agents are installed. The configuration parameter CSI_USER assigns the account used to run the Agent daemon or service. If the parameter is changed, the user account must not have a valid login shell. You must be logged in to a target UNIX/Linux machine as root.

NOTE If you have copied your custom configuration file from a previous installation, follow the optional step provided in this procedure. If you are using a custom configuration file, perform the installation in Silent Mode.

Installing the Agent on UNIX/Linux machines is a manual operation.

NOTE A Deployment Tool is available from Customer Support to assist you with the following process for UNIX/Linux. To use the tool, contact support; otherwise, follow the steps in the following process.

IMPORTANT To install the UNIX Agent on SUSE and Red Hat machines, you may need to disable or reconfigure firewalls.

Platforms Not Supported for Upgrade to 5.3 Agent

Installing or upgrading on the following platforms is supported only to the 5.1.3 UNIX Agent. You can install the 5.3 Agent; however these platforms are not tested with any additional 5.3 functionality.

Platform	Supported Agent Version	Agent File Name
AIX 4.3.3	5.1.3	CMAgent.5.1.0.AIX.4
Red Hat 2.1	5.1.3	CMAgent.5.1.0.Linux.2.1
Solaris 2.5	5.1.3	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.
Solaris 2.6	5.2.1	Contact VMware Customer Support if you are installing or upgrading the Agent on this platform.

Use the following steps to install the Agent.

1. Verify that the machine on which you intend to install the agent has enough free disk space. For more information, see the *VCM Hardware and Software Requirements Guide*.
2. When VCM is installed on the VCM Collector machine, the necessary Agent packages are created in the following locations:
   `\Program Files (x86)\VMware\VCM\Installer\Packages`
   or
   `\Program Files\VMware\VCM\Installer\Packages`.

   The following agent binaries are available in these locations for the associated operating systems:

Operating System Version	Agent Binary
Red Hat (Enterprise) Linux Edition (Version 2.1)	`CMAgent.<version>.Linux.2.1`
Red Hat (Enterprise) Linux Edition (Version 3.0, 4.0, 5.0, 5.1, 5.2, 5.3) SUSE Linux Enterprise Server (9, 10), Debian (4)	`CMAgent.<version>.Linux`
Solaris (Versions 8, 9, and 10 supported on Sparc)	`CMAgent.<version>.SunOS`
Solaris (Version 10 for x86)	`CMAgent.<version>.SunOS.x86.5.10`
HP-UX 11i Versions 1.0, 2.0, 3.0 (11.11, 11.23, and 11.31; Supported on PA-RISC)	`CMAgent.<version>.HP-UX.11.pa`
HP-UX 11i Version 2.0, 3.0 (11.23 and 11.31-Supported on Itanium)	`CMAgent.<version>.HPUX.11.ia64`
AIX Version 4.3.3	`CMAgent.<version>.AIX.4`
AIX Version 5L (5.1, 5.2, 5.3, and 6L (6.1))	`CMAgent.<version>.AIX.5`

3. Copy the installation package to the machine on which you want to install the agent. You can use **`ftp`**, **`sftp`**, or **`cp`** using an NFS share.

NOTE If you use ftp to copy the package to your machine, be sure to use binary mode.

4. Use `chmod u+x <filename>` to change the permissions on the agent binary file.
5. In the directory where you copied the file, execute the agent binary package to create the necessary directory structure and extract the files. The command and output will look similar to the following example, with differing file names depending on the operating system:

```
# ./CMAgent.<version>.SunOS
UnZipSFX 5.51 of 22 May 2004, by Info-ZIP (http://www.info-zip.org).
creating: CSIInstall/
creating: CSIInstall/packages/
inflating: CSIInstall/packages/Agent.1.0.SunOS
inflating: CSIInstall/packages/CFC.1.0.SunOS
inflating: CSIInstall/packages/ECMu.1.0.SunOS
inflating: CSIInstall/packages/ThirdParty.1.0.SunOS
inflating: CSIInstall/packages/cis.1.0.SunOS
extracting: CSIInstall/packages/package.sizes.SunOS
inflating: CSIInstall/packages/python.23.SunOS
creating: CSIInstall/scripts/
inflating: CSIInstall/scripts/checksum
inflating: CSIInstall/scripts/BootStrapInstall.sh
inflating: CSIInstall/scripts/AltSource_filesystem.sh
```

```
inflating: CSIInstall/scripts/AltSource_ftp.sh
inflating: CSIInstall/scripts/AltSource_rcp.sh
inflating: CSIInstall/scripts/AltSource_sftp.sh
inflating: CSIInstall/scripts/AltSource_wget.sh
extracting: CSIInstall/scripts/AltSourceCmd
inflating: CSIInstall/InstallCMAgent
inflating: CSIInstall/csi.config
inflating: CSIInstall/CMAgent.<version.OS>
creating: CSIInstall/.security/certificates/
inflating:CSIInstall/.security/certificates/<EnterpriseCertificate>
```

NOTE To force an overwrite of any existing files, include the -o option when executing the package. For example: `/CMAgent.<version>.SunOS -o`.

6. Change the directory to the location where the `InstallCMAgent` executable file was extracted. For example:
   `# cd <extractedpath>/CSIInstall`
7. Use the `ls -la` command to validate that the following files are in this directory:
   - **InstallCMAgent:** The installation script.
   - **csi.config:** The configuration file for the installation, where you can modify the installation options.
   - **packages:** Contains the installation packages.
   - **scripts:** Contains the scripts needed for the install.
8. To customize the settings for the installation variables, modify the installation configuration file, csi.config, and then save your changes. If this file has only read permissions set, you will need to give the file write permissions with the `chmod u+x csi.config` command. See the following installation options for details.

Installation Options with Default Values	Description
CSI_AGENT_RUN_OPTION	The Agent can be installed as a daemon process or installed to be run by inetd/xinetd/launchd. • A value of inetd will install the Agent for execution by inetd/xinetd/launchd. • A value of daemon will install the agent for execution as a daemon process.
CSI_NO_LOGIN_SHELL= +S:+A:+/sbin/noshell+/bin/false+ /sbin/false+/usr/bin/false +/sbin/nologin	The CSI_USER account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the CSI_USER has no-login shell. If your system has a valid no login shell that is not listed, then append a plus sign and add the no login shell to the list. The following describes the options available for this parameter: • +S means only for Solaris • +A means only for AIX • +H means only for HP-UX • +L means only for Linux • +D means only for Darwin (Mac OS X) • + means for all OS

Installation Options with Default Values	Description
CSI_CREATE_USER=Y Recommend keeping default value.	The user is being created. This value indicates whether or not the user is to be created. **Note:** When installing in trusted mode on HP-UX v1.0 (11.11), the user must already exist on the target machine. If you attempt to install and create the user, the installation of the Agent fails.
CSI_USER_ID=501 Recommend keeping default value.	This value is the integer value for the user ID of the created user.
CSI_USER_NO_LOGIN_ SHELL=/bin/false Recommend keeping default value.	Indicates the desired no-login shell value to use when creating the user.
CSI_USER_PRIMARY_ GROUP=csi_acct Recommend keeping default value.	Group name to use when creating a new user as the user's primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges.
CSI_CREATE_USER_ PRIMARY_GROUP=Y Recommend keeping default value.	This value indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501 Recommend keeping default value.	Create user's primary Group ID.
CSI_USER_USE_NEXT_ AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow the Group ID to be the next available local Group ID over CSI_USER_PRIMARY_GID.
CSI_USER=csi_acct Recommend keeping default value.	The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500 Recommend keeping default value.	The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.
CSI_CREATE_LOCAL_ GROUP=Y Recommend keeping default value.	Setting this option to Y allows the cfgsoft group to be created. This setting allows the system call to groupadd.

Installation Options with Default Values	Description
CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542 Recommend keeping default value.	This option specifies the port that the CM Agent will be listening on.
CSI_CREATE_LOCAL_SERVICE=Y Recommend keeping default value.	Setting CSI_CREATE_LOCAL_SERVICE to Y allows the system to create the local service (copy files to system directories).
CSI_REFRESH_INETD=Y Keep default value only if you are running your agent as inetd. If you are running your agent as a daemon, select CSI_REFRESH_INETD=N	Setting this option to allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX).
CSI_NICE=10 Recommend keeping default value.	This option sets the nice value for the agent listener process.
CSI_CERTIFICATE_PATH=	This option specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you can use this option to have the certificates put in the Agent location (VMware encourages you to install the Enterprise Certificates so that multiple Collectors collecting from the same set of Agents can be supported). If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	This option specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.
CSI_PARENT_DATA_DIRECTORY=/opt	This option specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/CMAgent/data
CSI_PARENT_LOG_DIRECTORY=default	This option specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use the following: • Linux - /var/log • AIX, HP-UX, and Solaris - /var/adm • Mac OS X- log ->private/var/log/CMAgent/log
CSI_KEEP_CSIINSTALL=N Recommend keeping default value.	After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

9. If you modified and saved the csi.config installation file, copy the saved csi.config to the extracted location. For example:
   `# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config`
10. Change the directory to the location where the `InstallCMAgent` executable file was extracted. For example:
    `# cd <extractedpath>/CSIInstall`
11. Execute `InstallCMAgent` in either silent mode or interactive mode, as described in the following options.

NOTE If you are using the custom configuration file, csi.config, proceed with the installation in Silent Mode.

Silent Mode:

If you execute `InstallCMAgent` in silent mode, the installation proceeds silently. It uses the values specified in `csi.config` without prompting for input. To run the installation in silent mode, enter:

```
# ./CSIInstall/InstallCMAgent -s
```

You might use this method if you have manually edited the **`csi.config`** file, if you have modified the **`csi.config`** file using the interactive method, or if you are using a custom configuration file that you saved from a previous agent installation.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

Interactive Mode:

If you execute the installation with no options, it runs in an interactive mode, prompting you to accept or change each parameter in the `csi.config` file.

NOTE When you use interactive mode, the `csi.config` file is modified.

To run the installation in interactive mode, enter:

```
# ./CSIInstall/InstallCMAgent
```

During the pre-installation stage of interactive mode, the check for a valid user (`CSI_USER`) is performed. If the user already exists (either the Administrator has manually added the account or is selecting an existing one), the following configuration values will not be requested (the questions will be skipped) by the installer:

- CSI_USER_NO_LOGIN_SHELL
- CSI_USER_PRIMARY_GROUP
- CSI_USER_PRIMARY_GID
- CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID

These prompts will be requested only when the `CSI_USER` user account is not found.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

NOTE If you selected inetd for CSI_AGENT_RUN_OPTION and xinetd (Linux only) is not running, the following error message will be displayed: SYSTEM_WARNING: xinetd is not running - the agent will be disabled until it is started. If this message appears, you must either start xinetd, or install the Agent as a daemon.

12. In addition to creating the necessary user and groups, and configuring the machine to run the Agent, the installation also creates a new directory in the <CSI_PARENT_DIRECTORY> named CMAgent (unless this directory was changed in the configuration). This directory contains the following files and subdirectories:

```
# ls -la /CSI_PARENT_DIRECTORY/CMAgent
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 Agent
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 CFC
-rw-rw---- 1 root cfgsoft 49993 Jul 2 17:34 CSIRegistry
-rw-rw---- 1 root cfgsoft 0 Jul 2 17:34 .CSIRegistry.lck
drwxrwx--- 3 csi_acct cfgsoft 4096 Jul 2 17:34 data
drwxrwx--- 3 root cfgsoft 4096 Jul 2 17:34 ECMu
drwxr-x--- 6 root cfgsoft 4096 Jul 2 17:34 install
lrwxrwxrwx 1 root root 20 Jul 2 17:34 log -> /var/log/CMAgent/log
dr-xr-x--x 3 root cfgsoft 4096 Jul 2 17:34 ThirdParty
drwxr-xr-x 2 root root 4096 Jul 2 17:34 uninstall
```

13. To verify the Agent was installed correctly and is listening on the port and ready to collect data, execute the following command:

```
# netstat -na | grep <port_number>
```

    Where the default <port_number> is typically 26542 for VCM installations.

14. For SUSE machines, after the installation completes, you may need to start xinetd using the command:

```
# ./etc/init.d/xinetd start
```

After you have installed the Agent on the UNIX/Linux machines, you are now ready to start collecting data from them. To do this, see "Performing a UNIX/Linux Collection". After selecting UNIX/Linux machines, note that UNIX/Linux data classes are available for collection.

Updates to UNIX Patch Assessment Content Affects UNIX Agent Performance

By default, VCM Patching checks for patch updates every 4 hours. The time required to perform this action depends on the amount of new content downloaded to the Collector during the update process.

When the UNIX patch assessment content is pushed out to the UNIX agents, the time required to execute jobs such as collections and remote commands will increase slightly. The time required will vary based on how much new or updated content needs to by synchronized between the Collector and the agent. This content push will happen when the first communication is initiated after installing the UNIX agent package, or when there is new patch content on the Collector that is applicable to the UNIX agent platform since the last agent/collector communication occurred.

Manually Uninstalling the UNIX/Linux Agent

Every installation generates an uninstall script, UninstallCMAgent, located at:
<path>/CMAgent/uninstall

Consider these points when uninstalling an Agent:

- The uninstall reverses all changes made by installation, however the installation log files are retained in `<AgentRoot>/install`. `<AgentRoot>` defaults to the CMAgent directory that was created during installation. Refer to "Locating the Agent Directory" if necessary.
- After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the CMAgent directory prior to running a new installation.

To uninstall the Agent, use the steps in the following procedure. If you want to use a custom configuration file, follow the optional step below before uninstalling the Agent.

1. (Optional) Copy `csi.config`, the file that contains all of the custom configuration settings, to a safe location. (This file can be found in `<path>/CMAgent/install`.)
2. Navigate up one level from the uninstall directory in the `CMAgent` directory.
3. Run the uninstall script using the following command:
   `# ./uninstall/UninstallCMAgent`

NOTE Consider these points when uninstalling an Agent:

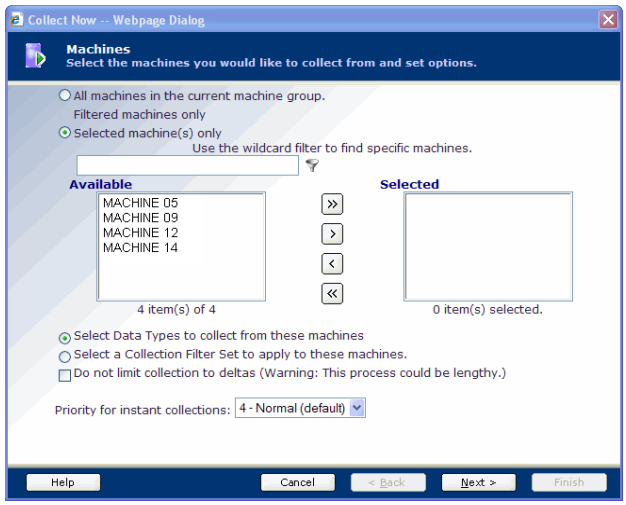
• The uninstall reverses all changes made by installation, however the installation log files are retained in `<AgentRoot>/install`. `<AgentRoot>` defaults to the CMAgent directory that was created during installation. Refer to "Locating the Agent Directory" later in this document if necessary.

• After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the CMAgent directory prior to running a new installation.

Performing a UNIX/Linux Collection

After the UNIX/Linux machines are added and licensed in VCM, and installed with the VCM Agent, you can perform a collection on those machines. The process for performing a UNIX/Linux collection is similar to other collections, including Windows, except that you select UNIX data types during your collection instead of Windows data types.

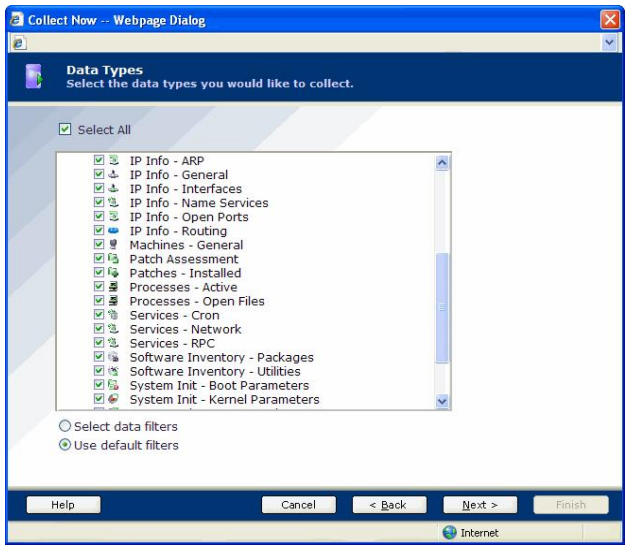
1. Click **Collect**, located on the Portal toolbar.
2. The **Collection Type** wizard page appears. Select **Machine Data**, and then click **OK**. The **Machines** page appears.


Collect Now -- Webpage Dialog
Machines
Select the machines you would like to collect from and set options.
All machines in the current machine group.
Filtered machines only
Selected machine(s) only
Use the wildcard filter to find specific machines.
Available
Selected
MACHINE 05
MACHINE 09
MACHINE 12
MACHINE 14
4 item(s) of 4
0 item(s) selected.
Select Data Types to collect from these machines
Select a Collection Filter Set to apply to these machines.
Do not limit collection to deltas (Warning: This process could be lengthy.)
Priority for instant collections:
4 - Normal (default)
Help
Cancel
< Back
Next >
Finish

3. Select the machine(s) from which you want to collect data. To select multiple machines, use **Shift-click** or **Ctrl-click**. Use the double arrow to move all visible machines to the selection window, 500 at a time. Leave the default options selected, then click **Next**.

NOTE UNIX Patch Assessment is automatically licensed and enabled if you have licensed your UNIX/Linux Agent machines. If you are upgrading from a previous version of VCM, you will need a new license file to access this functionality.

In order to view Patch Assessment data, click Select a Collection Filter Set to apply to these machines instead of the default collection options, and then select the UNIX Patch Assessment filter set. For more information, see the "UNIX Patch Assessment" Help topic.



4. The **Data Types** dialog box appears. Select the **Select All** check box, then confirm that the **Use default filters** option button is also selected. Click **Next**.
5. For initial collections, there should be no conflicts with previously scheduled or running jobs containing the same data types. Click **Finish**.
6. Verify that your collection job has completed before proceeding to the next step. To do so, click the **Jobs** button at the top of the Portal window to access the Jobs Summary.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your collection job by going to **Administration | Job Manager | History | Instant Collections | Past 24 Hours**. Refer to the online Help for additional detail regarding Jobs.

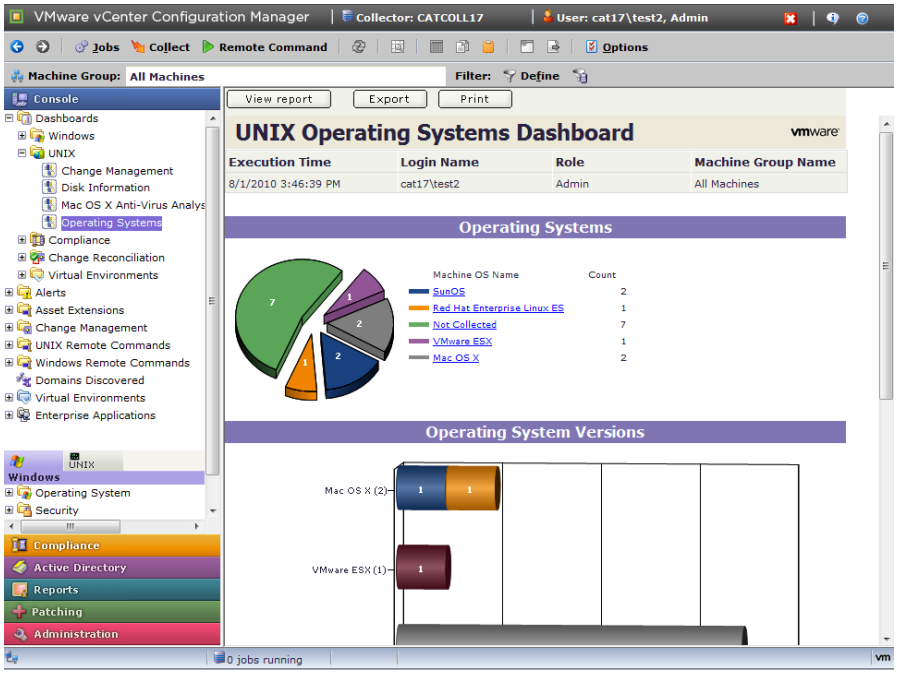
Exploring UNIX/Linux Collection Results

Now that you have performed an initial UNIX/Linux collection, you can explore that data in the Portal.

Dashboards

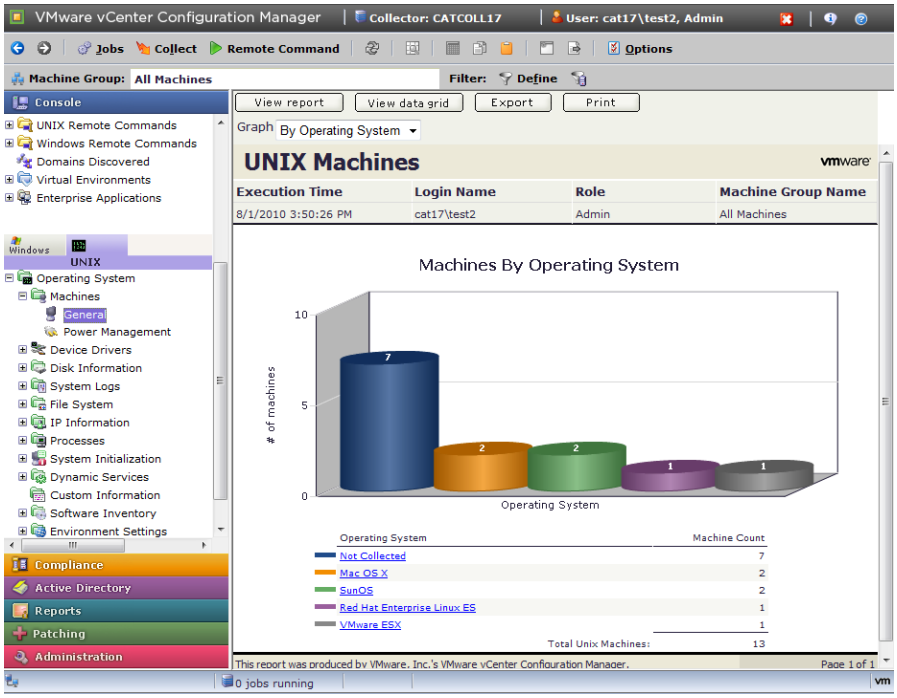
Each Dashboard is run only when the node is selected against the current data available in the CMDB for the machines in the active machine group. Therefore, Dashboard data is only current as of the time it was collected. In addition, it may take time for the data to display based on the volume or complexity of the data requested.

Begin by looking at the UNIX Operating System Dashboard under **Console | Dashboards | UNIX | Operating Systems**.



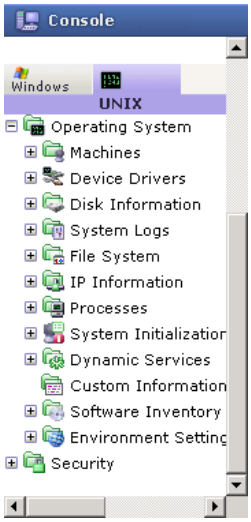
Note that several other UNIX Dashboards are also available. Take time to familiarize yourself with the remainder of the UNIX Dashboards. UNIX Collection Results are also available to you in a more "raw" format as well. This level of reporting is more relevant for day-to-day operations, troubleshooting, and analysis, and can be viewed in a Summary report or data grid format.

Look at your UNIX Operating System information by clicking the **UNIX** tab in the Console. Then, click **Operating System** | **Machines** | **General**.



When you select the node, you see a Summary Report as displayed above of the data type that you selected. Click **View data grid** to go directly to the data grid, or click an area of the Summary Report to filter the data before the data grid appears.

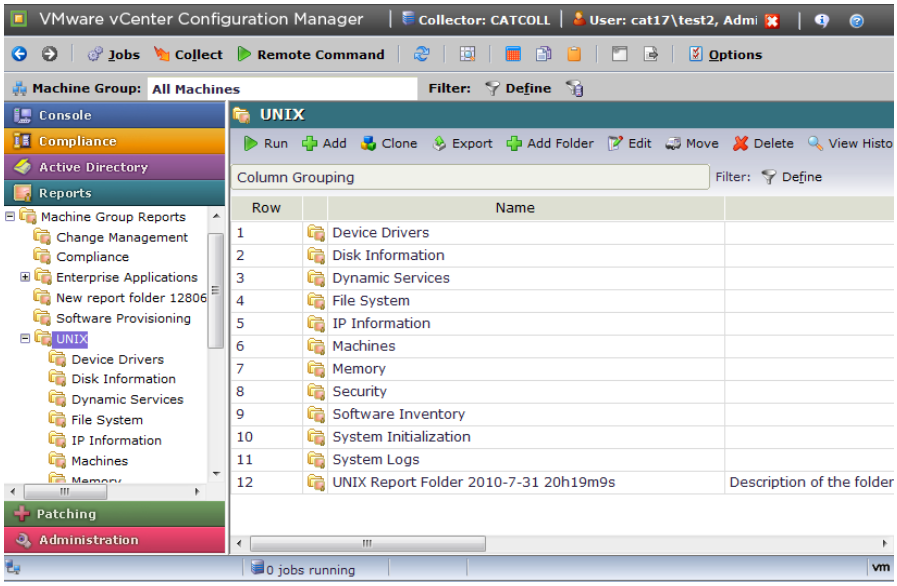
Several other categories (called "data classes") of information regarding your UNIX/Linux Collection are available under the UNIX tab.



The UNIX tab is where the remainder of your collected UNIX/Linux data is visible through the Portal.

Reports

An alternate way to view your collected UNIX/Linux data is by running VCM Reports or creating your own custom reports using VCM 's reporting wizard. To begin exploring the reporting functionality, go to the **Reports** slider, then click **Machine Group Reports** | **UNIX**.



Like Dashboards, Reports are run real time against the current data available in the CMDB for the machines in the active machine group, and therefore they are only as current as the time of the last collection. In addition, it may require time for the report to generate based on the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.

Compliance

You may now begin to check Compliance values for your collected data. To run a Compliance check, select the **Compliance** slider, then follow the steps described in the online Help to create rule groups, rules, filters, and templates.

Discover, License, and Install Mac OS X Machines

Getting Started with VCM for Mac OS X

The following steps must be performed before collecting data from Mac OS X machines:

1. Add Mac OS X machines.
2. License your Mac OS X machines.
3. Install the VCM Agent on your Mac OS X machines.
4. Perform an initial Mac OS X collection.
5. Explore the Mac OS X collection results.

These steps are explained in the following subsections.

Mac OS X machines are managed in conjunction with UNIX machines.

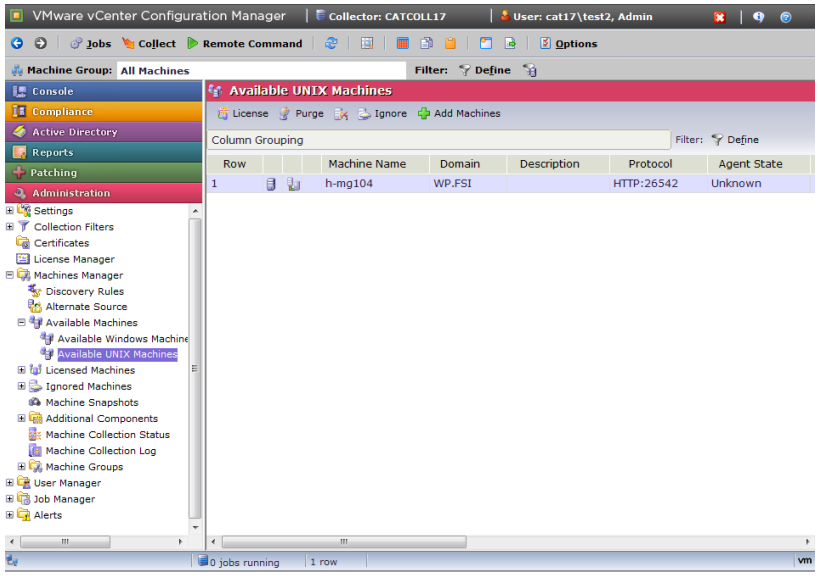
Adding Mac OS X Machines

Before you can collect data from your Mac OS X machines, they must be displayed in the Available UNIX Machines list located in the Portal under **Administration | Machines Manager | Available Machines**.

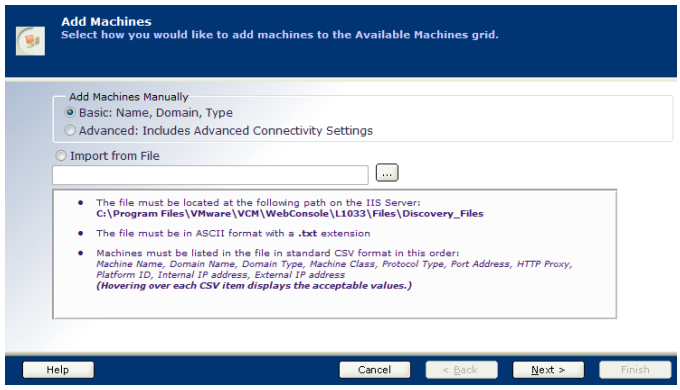
NOTE A Discovered Machines Import Tool (DMIT) is available from VMware Customer Support to assist you with the following process. This tool imports machines discovered by the Network Mapper (Nmap) into the configuration database. To use the tool, contact VMware Customer Support; otherwise, use the following process.

---

1. Click **Administration | Machines Manager | Available Machines | Available UNIX Machines**.

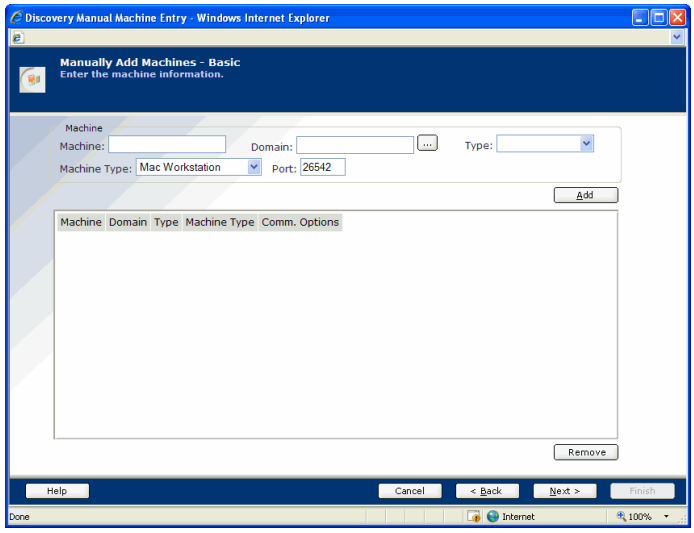


2. Click **Add Machines**. The **Add Machines** page appears.


Add Machines
Select how you would like to add machines to the Available Machines grid.
Add Machines Manually
Basic: Name, Domain, Type
Advanced: Includes Advanced Connectivity Settings
Import from File
The file must be located at the following path on the IIS Server:
C:\Program Files\VMware\VCM\WebConsole\L1033\Files\Discovery_Files
The file must be in ASCII format with a .txt extension
Machines must be listed in the file in standard CSV format in this order:
Machine Name, Domain Name, Domain Type, Machine Class, Protocol Type, Port Address, HTTP Proxy, Platform ID, Internal IP address, External IP address
(Hovering over each CSV item displays the acceptable values.)
Help
Cancel
< Back
Next >
Finish

3. Select **Basic**, and then click **Next**. The **Manually Add Machines - Basic** page appears.

NOTE When you expand your Mac OS X collections to a broader set of machines, you may want to use other methods to add your Mac OS X machines. Refer to the online Help for the advanced features such as importing from a file or using IP Discovery.



4. Enter the **Machine** and the **Domain**, and then select **DNS** for **Type**. For **Machine Type**, select the appropriate operating system. Modify the port number if you are not using the default.

   NOTE The port number specified must be the same number used when the Agent is installed on the managed Mac OS X machine.

5. Click **Add** to add the entry to the list.
6. Repeat for any other machines.
7. Click **Next** and accept the changes.

   NOTE If your Collector cannot resolve a host name with a DNS Server, be sure to use an IP address in place of a Machine name for your machines as you enter them.

Licensing Mac OS X Machines

When the Mac OS X machines are displayed in your Available UNIX Machines list, you may begin licensing these machines.

Use the following procedure to license your Mac OS X machines.

1. Click **Administration** | **Machines Manager** | **Available Machines** | **Available UNIX Machines**.

   NOTE Remember, discovered machines with an indeterminate **Machine Type** will not be licensed if they are included in your selection.

2. Select the machine(s) you want to license. To select multiple machines, use **Shift-click** or **Ctrl-click**.
3. Click **License**. The **Machines** page appears.
4. The machines that you specified appear in the **Selected** area. Add or remove machines from the list as needed.

5. Click **Next**. The **Product License Details** page appears.
6. The licensed machine count has increased by the number of machines that you have selected to license.
7. Click **Next**. The **Important** page appears.
8. Review the information.
9. Click **Finish**.

Installing the Agent on Mac OS X Machines

Before collecting data from your Mac OS X machines, you must install the VCM Agent on each licensed Mac OS X machine.

IMPORTANT The Collector should be installed before the Agents are installed. The configuration parameter CSI_USER assigns the account used to run the Agent daemon or service. If the parameter is changed, the user account must not have a valid login shell. You must be logged in to a target Mac OS X machine as root, or have sudo as root.

NOTE If you have copied your custom configuration file from a previous installation, follow the optional step provided in this procedure. If you are using a custom configuration file, perform the installation in Silent Mode.

Installing the Agent on Mac OS X machines is a manual operation. The Agent is packaged as a Universal Binary Installer.

Use the following steps to install the Agent.

1. Verify that the machine on which you intend to install the agent has enough free disk space. For more information, see the *VCM Hardware and Software Requirements Guide*.
2. When VCM is installed on the VCM Collector machine, the necessary Agent packages are created in the following locations:
   `\Program Files (x86)\VMware\VCM\Installer\Packages`
   or
   `\Program Files\VMware\VCM\Installer\Packages`.

   The following agent binaries are available in these locations for the associated operating systems:

Operating System Version	Agent Binary
Mac OS X (Version 10.4 and 10.5)	`CMAgent.<version>.Darwin`

3. Copy the installation package to the machine on which you want to install the agent. You can use **`ftp`**, **`sftp`**, or **`cp`** using an NFS share.

   NOTE If you use ftp to copy the package to your machine, be sure to use binary mode.

4. Use `chmod u+x <filename>` to change the permissions on the agent binary file.
5. In the directory where you copied the file, execute the agent binary package to create the necessary directory structure and extract the files. The command and output will look similar to the following example, with differing file names depending on the operating system:

```
# ./CMAgent.<version>.Darwin
UnZipSFX 5.51 of 22 May 2004, by Info-ZIP (http://www.info-zip.org).
creating: CSIInstall/

inflating: CSIInstall/CMAgent.5.1.0.Darwin.i386
inflating: CSIInstall/CMAgent.5.1.0.Darwin.ppc
inflating: CSIInstall/csi.config
inflating: CSIInstall/InstallCMAgent
```

NOTE To force an overwrite of any existing files, include the -o option when executing the package. For example: `/CMAgent.<version>.Darwin -o`.

6. Change the directory to the location where the `InstallCMAgent` executable file was extracted. For example:
   `# cd <extractedpath>/CSIInstall`
7. Use the `ls -la` command to validate that the following files are in this directory:
   - **InstallCMAgent:** The installation script.
   - **csi.config:** The configuration file for the installation, where you can modify the installation options.
   - **packages:** Contains the installation packages.
   - **scripts:** Contains the scripts needed for the install.
8. To customize the settings for the installation variables, modify the installation configuration file, csi.config, and then save your changes. If this file has only read permissions set, you will need to give the file write permissions with the `chmod u+x csi.config` command. See the following installation options for details.

Installation Options with Default Values	Description
CSI_AGENT_RUN_OPTION	The Agent can be installed as a daemon process or installed to be run by inetd/xinetd/launchd. • A value of inetd will install the Agent for execution by inetd/xinetd/launchd. • A value of daemon will install the agent for execution as a daemon process.
CSI_NO_LOGIN_SHELL= +S:+A:+/sbin/noshell+/bin/false+ /sbin/false+/usr/bin/false +/sbin/nologin	The CSI_USER account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the CSI_USER has no-login shell. If your system has a valid no login shell that is not listed, then append a plus sign and add the no login shell to the list. The following describes the option available for this parameter: • +S means only for Solaris • +A means only for AIX

Installation Options with Default Values	Description
	• +H means only for HP-UX • +L means only for Linux • +D means only for Darwin (Mac OS X) • + means for all OS
CSI_CREATE_USER=Y Recommend keeping default value.	The user is being created. This value indicates whether or not the user is to be created.
CSI_USER_ID=501 Recommend keeping default value.	This value is the integer value for the user ID of the created user.
CSI_USER_NO_LOGIN_ SHELL=/bin/false Recommend keeping default value.	Indicates the desired no-login shell value to use when creating the user.
CSI_USER_PRIMARY_ GROUP=csi_acct Recommend keeping default value.	Group name to use when creating a new user as the user's primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges.
CSI_CREATE_USER_ PRIMARY_GROUP=Y Recommend keeping default value.	This value indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501 Recommend keeping default value.	Create user's primary Group ID.
CSI_USER_USE_NEXT_ AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow the Group ID to be the next available local Group ID over CSI_USER_PRIMARY_GID.
CSI_USER=csi_acct Recommend keeping default value.	The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500 Recommend keeping default value.	The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.
CSI_CREATE_LOCAL_ GROUP=Y Recommend keeping default value.	Setting this option to Y allows the cfgsoft group to be created. This setting allows the system call to groupadd.

Installation Options with Default Values	Description
CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y Recommend keeping default value.	Setting this option to Y will allow this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542 Recommend keeping default value.	This option specifies the port that the CM Agent will be listening on.
CSI_CREATE_LOCAL_SERVICE=Y Recommend keeping default value.	Setting CSI_CREATE_LOCAL_SERVICE to Y allows the system to create the local service (copy files to system directories).
CSI_REFRESH_INETD=Y Keep default value only if you are running your agent as inetd. If you are running your agent as a daemon, select CSI_REFRESH_INETD=N	Setting this option to allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX). This option does not apply to Mac OS X.
CSI_NICE=10 Recommend keeping default value.	This option sets the nice value for the agent listener process.
CSI_CERTIFICATE_PATH=	This option specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you can use this option to have the certificates put in the Agent location (VMware encourages you to install the Enterprise Certificates so that multiple Collectors collecting from the same set of Agents can be supported). If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	This option specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.
CSI_PARENT_DATA_DIRECTORY=/opt	This option specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/CMAgent/data
CSI_PARENT_LOG_DIRECTORY=default	This option specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use the following: • Linux - /var/log • AIX, HP-UX, and Solaris - /var/adm • Mac OS X- log ->private/var/log/CMAgent/log
CSI_KEEP_CSIINSTALL=N Recommend keeping default value.	After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

9. If you modified and saved the csi.config installation file, copy the saved csi.config to the extracted location. For example:
   `# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config`
10. Change the directory to the location where the `InstallCMAgent` executable file was extracted. For example:
    `# cd <extractedpath>/CSIInstall`
11. Execute `InstallCMAgent` in either silent mode or interactive mode, as described in the following options.

NOTE If you are using the custom configuration file, csi.config, proceed with the installation in Silent Mode.

Silent Mode:

If you execute `InstallCMAgent` in silent mode, the installation proceeds silently. It uses the values specified in `csi.config` without prompting for input. To run the installation in silent mode, enter:

```
# ./CSIInstall/InstallCMAgent -s
```

You might use this method if you have manually edited the **`csi.config`** file, if you have modified the **`csi.config`** file using the interactive method, or if you are using a custom configuration file that you saved from a previous agent installation.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

Interactive Mode:

If you execute the installation with no options, it runs in an interactive mode, prompting you to accept or change each parameter in the `csi.config` file.

NOTE When you use interactive mode, the `csi.config` file is modified.

To run the installation in interactive mode, enter:

```
# ./CSIInstall/InstallCMAgent
```

During the pre-installation stage of interactive mode, the check for a valid user (`CSI_USER`) is performed. If the user already exists (either the Administrator has manually added the account or is selecting an existing one), the following configuration values will not be requested (the questions will be skipped) by the installer:

- CSI_USER_NO_LOGIN_SHELL
- CSI_USER_PRIMARY_GROUP
- CSI_USER_PRIMARY_GID
- CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID

These prompts will be requested only when the `CSI_USER` user account is not found.

NOTE The User and the Group are created in the local directory service storage.

When the silent installation completes, a summary of the installation process and status is displayed. Make sure the installation completed without errors.

You can check the installation status at anytime by viewing the installation log file at `<CSI_PARENT_DIRECTORY>/log/install.log`.

12. In addition to creating the necessary user and groups, and configuring the machine to run the Agent, the installation also creates a new directory in the `<CSI_PARENT_DIRECTORY>` named `CMAgent` (unless this directory was changed in the configuration). This directory contains the following files and subdirectories:

```
# ls –la /CSI_PARENT_DIRECTORY/CMAgent
```

```
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 Agent
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 CFC
-rw-rw---- 1 root cfgsoft 49993 Jul 2 17:34 CSIRegistry
-rw-rw---- 1 root cfgsoft 0 Jul 2 17:34 .CSIRegistry.lck
drwxrwx--- 3 csi_acct cfgsoft 4096 Jul 2 17:34 data
drwxrwx--- 3 root cfgsoft 4096 Jul 2 17:34 ECMu
drwxr-x--- 6 root cfgsoft 4096 Jul 2 17:34 install
lrwxrwxrwx 1 root root 20 Jul 2 17:34 log -> /var/log/CMAgent/log
dr-xr-x--x 3 root cfgsoft 4096 Jul 2 17:34 ThirdParty
drwxr-xr-x 2 root root 4096 Jul 2 17:34 uninstall
```

13. To verify the Agent was installed correctly and is listening on the port and ready to collect data, execute the following command:

    ```
    # netstat -na | grep <port_number>
    ```

    Where the default <port_number> is typically 26542 for VCM installations.

After you have installed the Agent on the Mac OS X machines, you are now ready to start collecting data from them. To do this, see "Performing a Mac OS X Collection". After selecting Mac OS X machines, note that Mac OS X data classes are available for collection.

Updates to UNIX Patch Assessment Content Affects UNIX Agent Performance

By default, VCM Patching checks for patch updates every 4 hours. The time required to perform this action depends on the amount of new content downloaded to the Collector during the update process.

When the UNIX patch assessment content is pushed out to the UNIX agents, the time required to execute jobs such as collections and remote commands will increase slightly. The time required will vary based on how much new or updated content needs to by synchronized between the Collector and the agent. This content push will happen when the first communication is initiated after installing the UNIX agent package, or when there is new patch content on the Collector that is applicable to the UNIX agent platform since the last agent/collector communication occurred.

Manually Uninstalling the Mac OS X Agent

Every installation generates an uninstall script, UninstallCMAgent, located at:
`<path>/CMAgent/uninstall`

Consider these points when uninstalling an Agent:

- The uninstall reverses all changes made by installation, however the installation log files are retained in `<AgentRoot>/install`. `<AgentRoot>` defaults to the CMAgent directory that was created during installation. Refer to "Locating the Agent Directory" if necessary.
- After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the CMAgent directory prior to running a new installation.

To uninstall the Agent, use the steps in the following procedure. If you want to use a custom configuration file, follow the optional step below before uninstalling the Agent.

1. (Optional) Copy `csi.config`, the file that contains all of the custom configuration settings, to a safe location. (This file can be found in `<path>/CMAgent/install`.)
2. Navigate up one level from the uninstall directory in the `CMAgent` directory.
3. Run the uninstall script using the following command:
   `# ./uninstall/UninstallCMAgent`

NOTE Consider these points when uninstalling an Agent:

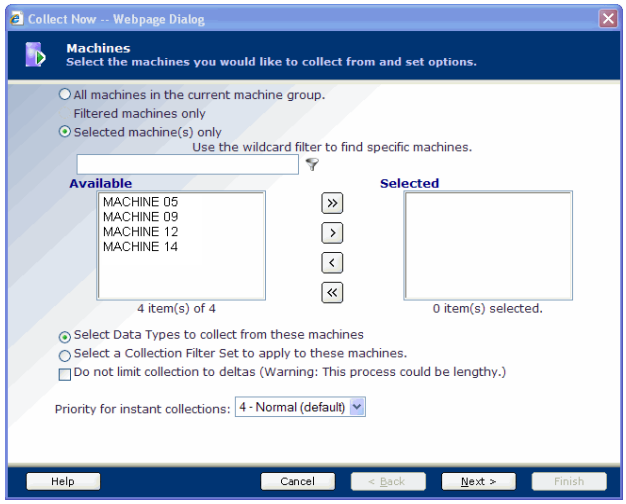
• The uninstall reverses all changes made by installation, however the installation log files are retained in `<AgentRoot>/install`. `<AgentRoot>` defaults to the CMAgent directory that was created during installation. Refer to "Locating the Agent Directory" later in this document if necessary.

• After executing `UninstallCMAgent`, VMware recommends that you delete the remaining the CMAgent directory prior to running a new installation.

Performing a Mac OS X Collection

After the Mac OS X machines are added and licensed in VCM, and installed with the VCM Agent, you can perform a collection on those machines. The process for performing a Mac OS X collection is similar to other collections, including Windows, except that you select Mac OS X data types during your collection instead of Windows data types.

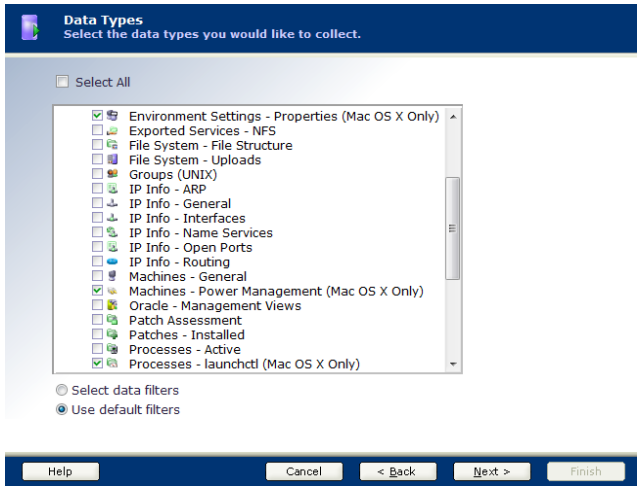
1. Click **Collect**, located on the Portal toolbar.
2. The **Collection Type** wizard page appears. Select **Machine Data**, and then click **OK**. The **Machines** page appears.


Collect Now -- Webpage Dialog
Machines
Select the machines you would like to collect from and set options.
All machines in the current machine group.
Filtered machines only
Selected machine(s) only
Use the wildcard filter to find specific machines.
Available
Selected
MACHINE 05
MACHINE 09
MACHINE 12
MACHINE 14
4 item(s) of 4
0 item(s) selected.
Select Data Types to collect from these machines
Select a Collection Filter Set to apply to these machines.
Do not limit collection to deltas (Warning: This process could be lengthy.)
Priority for instant collections:
4 - Normal (default)
Help
Cancel
< Back
Next >
Finish

3. Select the machine(s) from which you want to collect data. To select multiple machines, use **Shift-click** or **Ctrl-click**. Use the double arrow to move all visible machines to the selection window, 500 at a time. Leave the default options selected, then click **Next**.

NOTE UNIX Patch Assessment is automatically licensed and enabled if you have licensed your UNIX/Linux Agent machines. If you are upgrading from a previous version of VCM, you will need a new license file to access this functionality.

In order to view Patch Assessment data, click Select a Collection Filter Set to apply to these machines instead of the default collection options, and then select the UNIX Patch Assessment filter set. For more information, see the "UNIX Patch Assessment" Help topic.



The data classes and filters for Mac OS X include the following:

- Machines | General
- File System | File Structure
- System Logs | syslog events
- IP Information | General
- IP Information | Routing
- IP Information | Interfaces (IF)
- IP Information | Open Ports
- Security | Users | Current
- Security | Users | Information
- Security | Groups
- Custom Information – subset of CITs
- Properties files (.plist)
- Machines | General
- File System | File Structure
- System Logs | syslog events
- IP Information | General
- IP Information | Routing
- IP Information | Interfaces (IF)
- IP Information | Open Ports
- Security | Users | Current
- Security | Users | Information
- Security | Groups
- Custom Information – subset of CITs
- Properties files (.plist)

4. The **Data Types** dialog box appears. Select the **Select All** check box, then confirm that the **Use default filters** option button is also selected. Click **Next**.
5. For initial collections, there should be no conflicts with previously scheduled or running jobs containing the same data types. Click **Finish**.
6. Verify that your collection job has completed before proceeding to the next step. To do so, click the **Jobs** button at the top of the Portal window to access the Jobs Summary.

NOTE You can also verify jobs for the past 24 hours if you think that you may have missed your collection job by going to **Administration | Job Manager | History | Instant Collections | Past 24 Hours**. Refer to the online Help for additional detail regarding Jobs.

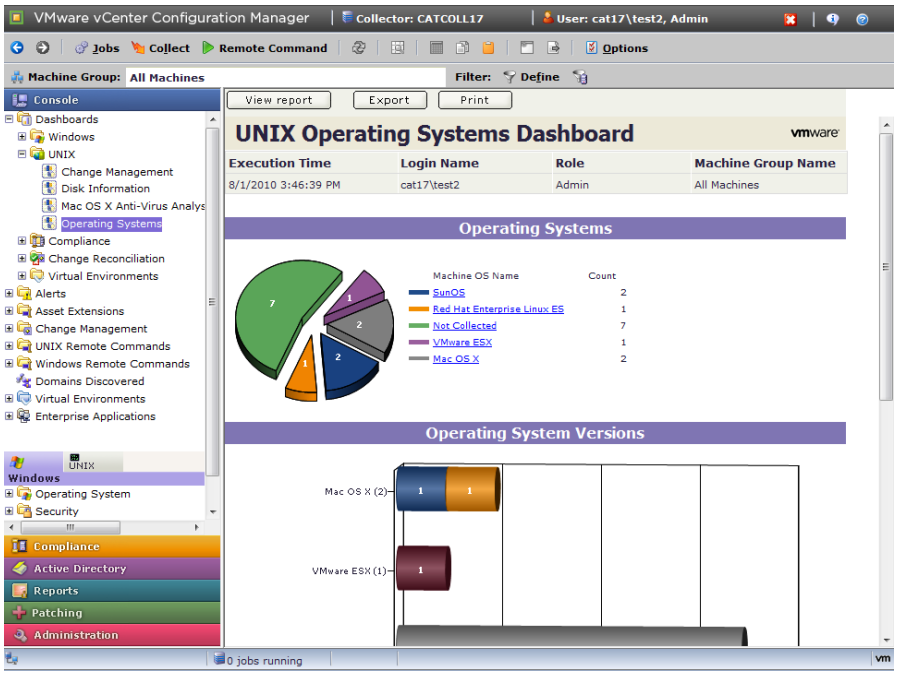
Exploring Mac OS X Collection Results

Now that you have performed an initial Mac OS X collection, you can explore that data in the Portal.

Dashboards

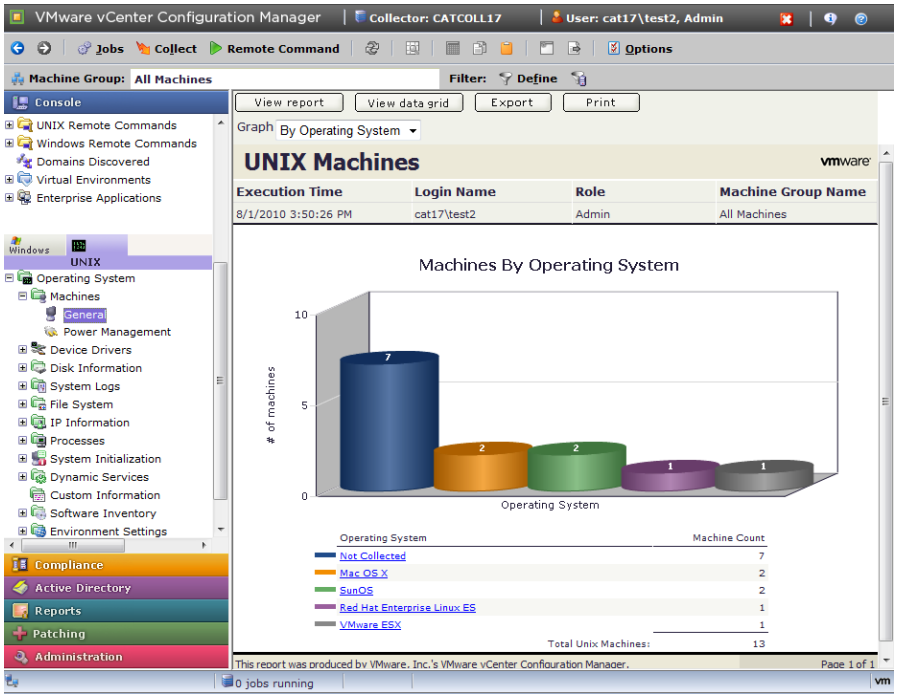
Mac OS X data is displayed in the UNIX Dashboards. Each Dashboard is run only when the node is selected against the current data available in the CMDB for the machines in the active machine group. Therefore, Dashboard data is only current as of the time it was collected. In addition, it may take time for the data to display based on the volume or complexity of the data requested.

To view Mac OS data, begin by looking at the UNIX Operating System Dashboard under **Console** | **Dashboards** | **UNIX** | **Operating Systems**.



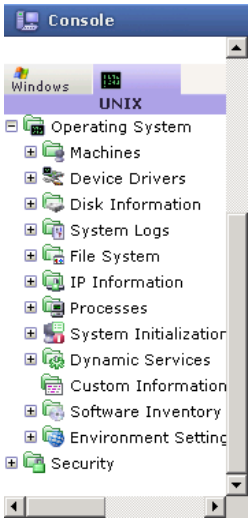
Note that several other UNIX Dashboards are also available. Take time to familiarize yourself with the remainder of the UNIX Dashboards. UNIX Collection Results are also available to you in a more “raw” format as well. This level of reporting is more relevant for day-to-day operations, troubleshooting, and analysis, and can be viewed in a Summary report or data grid format.

Look at your Mac OS X Operating System information by clicking the **UNIX** tab in the Console. Then, click **Operating System** | **Machines** | **General**.



When you select the node, you see a Summary Report as displayed above of the data type that you selected. Click **View data grid** to go directly to the data grid, or click an area of the Summary Report to filter the data before the data grid appears.

Several other categories (called "data classes") of information regarding your Mac OS X Collection are available under the UNIX tab.

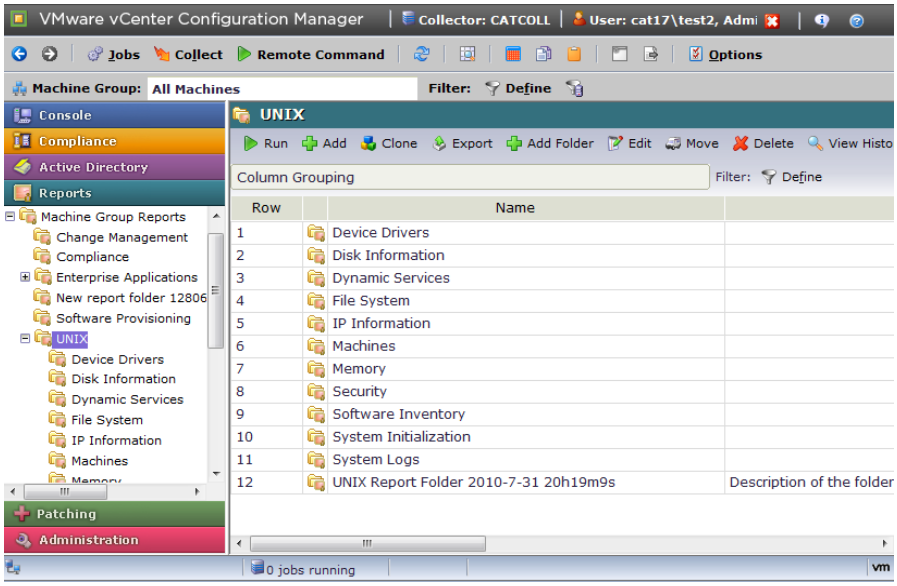


The UNIX tab is where the remainder of your collected Mac OS X data is visible through the Portal.

NOTE The displayed data is based on the collected Mac OS X data classes, also known as data types. See the Help for a list of currently collected data types.

Reports

An alternate way to view your collected Mac OS X data is by running VCM Reports or creating your own custom reports using VCM 's reporting wizard. To begin exploring the reporting functionality, go to the **Reports** slider, then click **Machine Group Reports** | **UNIX**.



Like Dashboards, Reports are run real time against the current data available in the CMDB for the machines in the active machine group, and therefore they are only as current as the time of the last collection. In addition, it may require time for the report to generate based on the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.

Compliance

You may now begin to check Compliance values for your collected data. To run a Compliance check, select the **Compliance** slider, then follow the steps described in the online Help to create rule groups, rules, filters, and templates.

Discover, License, and Collect Oracle Data from UNIX Machines

Welcome to VCM for Oracle. Now that you have installed VCM successfully, use the following steps to discover, collect, and work with Oracle data in VCM.

When getting started, you will first add the Oracle Instance, and then configure the Oracle Collection User account for database access. If you will be creating the Oracle Collection User account on Oracle 10g, see the following section about setting permissions on this account.

NOTE VCM uses the OS-authenticated Oracle Collection User account to connect to the Oracle database so that Oracle collections can be performed. This account can be created in two ways: 1) using the **Config User** action, or 2) using the **Oracle Account Setup remote command**.

To get started with VCM for Oracle, follow these steps:

1. Add UNIX machines hosting Oracle and install the Agent.
2. Discover Oracle Instances.
3. Create the Oracle Collection User Account.
4. Perform an Oracle collection.
5. Explore Oracle collection results.
6. Explore reference information about Oracle.

For instructions on removing access to the Oracle database, see "Removing Access to the Oracle Database" on page 112.

Adding UNIX Machines Hosting Oracle and Installing the Agent

1. Add UNIX machines in **Administration | Machines Manager | Available Machines | Available UNIX Machines | Add Machines**.
2. License UNIX machines in **Administration | Machines Manager | Available Machines | Available UNIX Machines | License**.
3. Install the Agent on one or more UNIX machines. See "Installing the Agent on UNIX/Linux Machines" on page 83.

Discovering Oracle Instances

An Oracle Instance is a structure of memory and background processes used to interact with the Oracle database to access data. The Oracle Instance contains stored information that is shared by various Oracle processes, and private information used for particular processes.

The Oracle database includes the physical files used to store information, including database engine data files, containing database metadata control files, and log files of data changes for backup and recovery.

Use this view to add and configure an Oracle Instance on a machine. After an Oracle Instance has been added, you must configure the database access for the Oracle Collection User that VCM will use to collect from that Oracle Instance.

TIP After you have configured the Oracle Instance, use the **Config User** action to configure database access for the Oracle Collection User account.

---

1. Run a full collection on UNIX machines using the **Machines - General** and **Oracle - Management Views** data types. This process includes a discovery of Oracle Instances from the oratab file on Solaris machines. See "Performing a UNIX/Linux Collection" on page 90 for more information about running collections on UNIX machines.
2. To edit or to manually add an Oracle Instance, see "Adding Oracle Instances" on page 109.

Adding Oracle Instances

During the collection performed in the previous section, the Agent retrieves **ORACLE_HOME**, **ORACLE_SID** and **Oracle Software Owner** from the oratab file, and displays the data in VCM. Review the list of Oracle instances populated in **Administration | Machines Manager | Additional Components | VCM for Oracle**.

Add an Oracle Instance

To add an Oracle Instance to a UNIX machine, follow these steps:

1. In **Administration** | **Machines Manager** | **Additional Components** | **VCM for Oracle**, click **Add**. The **Add Oracle Instances** wizard opens.
2. Select the machine(s) on which you want to add an Oracle Instance. Click **Next**. The **Configuration Values** wizard page appears.

   NOTE On UNIX Machines, a **Machines - General** collection is necessary to see machines in the wizard. Supported UNIX machines displayed in the wizard include Solaris versions 9 and 10.

3. Enter the configuration values for each Oracle Instance (**Oracle SID**, **Oracle Home**, **Oracle SW Owner**, **DBA Group**, and **Oracle Collection User**). See the VCM for Oracle data grid for definitions of these values. Click **Next**, and then click **Finish**.

   NOTE If VCM already contains the machine and **Oracle SID** that are added, a conflict screen appears showing the machine and Instance that are in conflict. If other values exist, which were changed for the conflicting machine and Instance, the "Update the existing Instances" check box appears. If you want to update the existing Instance, check this box. Otherwise, the Instance will not be updated.

Edit an Oracle Instance

1. In **Administration** | **Machines Manager** | **Additional Components** | **VCM for Oracle**, click **Edit**. The Edit Oracle Instances wizard opens.
2. Select the machine(s) on which you want to edit an existing Oracle Instance. Click **Next**. The **Configuration Values** wizard page appears.
3. Check the box next to a configuration value you want to modify. See the VCM for Oracle data grid for definitions of these values. Click **Next**, and then click **Finish**.

Creating the Oracle Collection User Account

After the Oracle Instance has been added, use one of these methods to configure the Oracle Collection User account for database access to Oracle Instances:

- Create the Oracle Collection User Account with the Config User Action
- Create the Oracle Collection User Account with a Remote Command

If you are working with Oracle 10g, see "Permissions for Oracle Collection User Account on Oracle 10g" on page 113 for more information.

Creating the Oracle Collection User Account with the Config User Action

The **Configure Oracle User** action configures database access to Oracle Instances for the Oracle user. You can create the Oracle Collection User account on Oracle 10g.If you are working with Oracle 10g, see "Permissions for Oracle Collection User Account on Oracle 10g" on page 113 for more information.

To create the OS-authenticated Oracle Collection User account with the **Config User** action, follow these steps:

1. Click **Config User**. The **Select Oracle Instances** wizard opens.
2. Select one or more **Oracle Instances**. You can set a filter on these items. Click **Next**, and then click **Finish**.

   Filter the Oracle Instances based on:

- Machine Name
- Oracle Home (Collected)
- Oracle Home (Override)
- Oracle SID
- Oracle Software Owner (Override)
- Oracle Software Owner (Override)
- Oracle User

3. In the **Schedule** wizard page, set the job timing schedule. You can run the action immediately or schedule it to run later. Click **Next**.

You can remove access to the Oracle database. "Removing Access to the Oracle Database" on page 112

Creating the Oracle Collection User Account with a Remote Command

VCM must have the appropriate Oracle database access to collect data from Oracle Instances. VCM uses the Oracle Collection User account to connect to the Oracle database so that Oracle collections can be performed.

The preferred method is to create the Oracle Collection User account using the Config User action. Or, you can use the UNIX Remote Command, as described in the instructions below.

NOTE You can add Oracle Instances and create Oracle Collection User accounts on 64-bit and 32-bit supported UNIX machines.

For instructions on removing access to the Oracle database, see Removing Access to the Oracle Database.

Setting Account Permissions on Oracle 10g

If you will be creating the Oracle Collection User account on Oracle 10g, see "Permissions for Oracle Collection User Account on Oracle 10g" on page 113 for information about setting permissions on this account.

Create the Oracle Collection User Account with a Remote Command

To create the OS-authenticated Oracle Collection User account with a remote command, follow these steps:

1. Edit the **Install Oracle Collection User Account** remote command in **Console | UNIX Remote Commands | Oracle Account Setup**. Click the **Install Oracle Collection User Account** remote command, and then click **Edit**. The Remote Commands wizard appears.
2. Review the default values for the remote command and edit them with the correct values for your environment. Example values are shown here.
   a. Type the **ORACLE_SID** (Oracle instance).
   b. Type the **ORACLE_HOME** (path).
   c. Type the **ORACLE_COLLECTION_USER_ACCOUNT**. If an account is not specified, the **ORACLE_COLLECTION_USER_ACCOUNT** named "**csiora**" will be created by default.

d. Type the **ORACLE_SOFTWARE_OWNER_ACCOUNT**. If left blank, VCM will attempt to derive it by determining the owner of the **ORACLE_HOME** directory. This account is used to log into the Oracle database to create the Oracle OS-authenticated User account (Oracle Collection User account).

3. On the **Files Wizard** page, select the **InstallOracleCollectionUserAccount.sh** file.
4. Run the job as root. If desired, select the option of storing results on the VCM Collector.
5. Select the machine(s) on which to create the Oracle Collection User account.
6. Select to run the remote command now. As the remote command is running, the following actions will be performed:
    a. Action will be run with root privileges (for example, **Setuid – RunHigh**).
    b. If the local user does not exist, a non-privileged OS user account will be created and the password will be locked.
    c. Switch or "**su**" to the **ORACLE_SOFTWARE_OWNER_ACCOUNT** that was provided.
    d. Connect to the Oracle database using the sqlplus binary.
    e. Create the Oracle OS-authenticated User account if it does not exist.
    f. Grant the Oracle OS-authenticated User account the **SELECT_CATALOG** role (privilege necessary for accessing data dictionary views and packages).
    g. If the option was chosen to store results in a local directory, the job status (success or failure) will be returned here.

If you no longer want to collect from an Oracle database, you can remove access to the Oracle database.

Removing Access to the Oracle Database

To remove access to the Oracle database, follow these steps:

1. Edit the **Uninstall Oracle Collection User Account** remote command in **Console | UNIX Remote Commands | Oracle Account Setup**. Click the **Uninstall Oracle Collection User Account** remote command, and then click **Edit**. The Remote Commands wizard appears.
2. Review the default values for the remote command and edit them with the correct values for your environment. Example values are shown here.
    a. Enters the **ORACLE_SID** (Oracle instance)
    b. Enter the **ORACLE_HOME** (path).
    c. Enters the **ORACLE_COLLECTION_USER_ACCOUNT** that should be removed.
    d. Either enter the **ORACLE_SOFTWARE_OWNER_ACCOUNT**. If left blank, VCM will attempt to derive it by determining the owner of the **ORACLE_HOME** directory.
3. In the Files wizard page, select the **UninstallOracleCollectionUserAccount.sh** file.
4. Run the job as root. If desired, select the option of storing results on the VCM Collector.
5. Select the machine(s) on which to remove the Oracle account.
6. Select to run the remote command now. As the remote command is running, the following actions will be performed:
    a. Action will be run with root privileges (for example, **Setuid - RunHigh**)
    b. The non-privileged OS user account will be deleted.
    c. Switch or "**su**" to the **ORACLE_SOFTWARE_OWNER_ACCOUNT** that was provided.

d. Connect to the Oracle database using the sqlplus binary.

e. The Oracle OS-authenticated account will be removed for Oracle database.

f. If the option was chosen to store results in a local directory, the job status (success or failure) will be returned here.

1 After the Oracle OS-authenticated account is removed, VCM will not be able to collect Oracle data unless an account is recreated.

Permissions for Oracle Collection User Account on Oracle 10g

For Oracle 10g installations, permissions are set by default to prevent users who are not part of the Oracle DBA Group from accessing and executing files in the Oracle Home directory. Because the Oracle Collection User account typically does not belong to the Oracle DBA Group, problems may arise when executing SQL*Plus using the Oracle Collection User account.

Consequently, if this account does not have access to the necessary directories and files in Oracle Home to execute SQL*Plus, Oracle - Management View data will not be collected. Therefore, you must ensure that the Oracle Collection User account that is created has appropriate access to the required binaries.

For the Oracle Collection User account to execute SQL*Plus, you must grant Oracle directories read/read-execute permission grant Oracle directories read/read-execute permission.

Grant Permission to the Oracle Collection User Account to Execute SQL*Plus

The following Oracle directories must be granted permission:

`chmod o+rx <top level oracle install>` (for example, /opt/oracle, /oracle, etc.)

```
- repeat for every directory level from the top level install down to
$ORACLE_HOME

- Example: If the top level is /oracle, and $ORACLE_HOME is
/oracle/app/product/10.20.0/db_1, then:

chmod o+rx /oracle/app

chmod o+rx /oracle/app/product

chmod o+rx /oracle/app/product/10.20.0

chmod o+rx /oracle/app/product/10.20.0/db_1

- Continue, after verifying the $ORACLE_HOME environment variable is set:

chmod o+rx $ORACLE_HOME

chmod o+rx $ORACLE_HOME/jdbc

chmod o+rx $ORACLE_HOME/jdbc/lib

chmod o+rx $ORACLE_HOME/ldap

chmod o+rx $ORACLE_HOME/ldap/mesg

chmod o+r $ORACLE_HOME/ldap/mesg/*

chmod o+rx $ORACLE_HOME/network

chmod o+rx $ORACLE_HOME/network/admin

chmod o+rx $ORACLE_HOME/sqlplus

chmod o+rx $ORACLE_HOME/sqlplus/mesg
```

```
chmod o+r $ORACLE_HOME/sqlplus/mesg/sp1us.msb
chmod o+r $ORACLE_HOME/sqlplus/mesg/sp2us.msb
chmod o+rx $ORACLE_HOME/nls
chmod o+rx $ORACLE_HOME/nls/data
chmod o+r $ORACLE_HOME/nls/data/lx1boot.nlb
chmod o+r $ORACLE_HOME/nls/data/*
chmod o+rx $ORACLE_HOME/oracore
chmod o+rx $ORACLE_HOME/oracore/zoneinfo
chmod o+r $ORACLE_HOME/oracore/zoneinfo/timezlrg.dat
```

Alternate Approach to Modify Permissions in Oracle

Oracle has provided a change permissions script, `changePerm.sh`, which is included with most Oracle 10g installations. This script is typically located in `$ORACLE_HOME/install` by default.

An alternate approach is to run the `changePerm.sh` script. Running this script relaxes permissions on several directories and files in Oracle Home so that users who are not part of the Oracle DBA Group can access parts of Oracle, such as SQL*Plus. However, because running this script grants every UNIX account read and execute permissions to most, if not all, directories and files in Oracle Home, this option is not recommended.

Performing an Oracle Collection

Run a collection on UNIX machines using the **Oracle - Management Views** data class. Any fields that were modified in the Oracle administration data grid will be used in collections of data performed during the discovery process.

NOTE To limit the amount of data stored in the change log, from collections performed using the **Oracle - Management Views** data class before the **Oracle Collection User account** was defined, ensure that you check the option, **Do not limit collection to deltas** for this collection.

Exploring Oracle Collection Results

After collecting Oracle data, view the data in the **Management Views** in **Console | Enterprise Applications | Oracle | Management Views**.

The **Oracle Management Views** display security information, including users, roles, and privileges; configuration settings; and database parameters for Oracle Instances. The data in these views is collected from views within each Oracle Instance on supported Solaris machines. Each **Oracle Management View** displays the Oracle data, the Machine Name, Instance Name (Oracle SID), and the date the data was last updated.

Reference Information about Oracle

For a list of supported Solaris machines, see the *VCM Hardware/Software Requirements Guide*.

The following views show additional VCM data. For additional information, see the online Help.

- VCM for Oracle data grid in **Administration | Machines Manager | Additional Components | VCM for Oracle**
- Management Views in **Console | Enterprise Applications | Oracle | Management Views**

- Oracle Management View Data Types
- Oracle Mgmt View – Audit Table Privs

For Oracle 9i Online Documentation, see:
(http://www.oracle.com/pls/db92/db92.docindex?remark=homepage)

For Oracle 10g Online Documentation, see:
(http://www.oracle.com/pls/db102/homepage)

Customize VCM for your Environment

You have now completed the preliminary setup procedures. For more information about how to use VCM, refer to online Help, available in the Portal. As always, if you have any questions or problems using VCM, contact VMware Customer Support. Customization of your environment is essential to fine-tune the visibility of configuration information so that the policies you develop and the actions you take are appropriate for your IT infrastructure.

As you learn more about VCM, it is highly advised that you take advantage of the organization of machines in your environment by creating a relevant machine group structure. These machine groups allow you to manage specific machines in your environment (for example, all SQL Servers in Ohio) and to apply specific changes or create Roles/Rules for those machines independently of other machines in your environment. This also ensures that access to critical machines can be restricted to appropriate personnel with rights to VCM. Additionally, you can customize the following options specifically for your environment:

- **Alerts:** The alerting system allows you to define the objects and types of changes that you are alerted to when they are detected in VCM. For example, you could set up an alert to notify you if a registry setting changes in your environment. Refer to the online Help on Alerts for more information.
- **Collection Filters and Filter Sets:** Use Collection Filters to specify the data that you want to collect from the machines that VCM manages. A default Collection Filter is provided for each data type. You can choose to add custom Collection Filters that are specific to your enterprise. Filters can be applied during Instant Collections and during Scheduled Collections if they are included as part of a filter set. Once you have created Collection Filters, organize them into Filter Sets. You might want to create specific Filter Sets or Filter Set Groups for different Machine Groups. Filter Sets can also be applied during Instant or Scheduled Collections. Refer to the online Help about Collection Filters for more information.
- **Compliance Templates and Rule Groups:** Use Compliance Templates and Rule Groups to define desired settings and check whether or not machines match those ideals. VCM comes with pre-packaged templates and rules that let you immediately start checking your machines' compliance to regulatory, industry, and vendor standards. Refer to the online Help for more information. Additionally, other compliance packages are available from VMware that can be imported into VCM post-installation. Refer to Import/Export and Content Wizard for more information.
- **Reports:** Use Reports to create and print tailored reports of information not shown specifically in VCM. VCM comes with pre-packaged reports that you can run as soon as you have collected data from your licensed machines. Refer to the online Help for more information.
- **Roles and Rules:** VCM roles and access rules work together to control a user's access to VCM. For example, you may create a role that allows a user to view all data, but not allow the user to make changes to the environment. Alternatively, you can create a role that can be used only to run certain reports, or a role that allows unlimited access to a single Machine Group. Refer to the online Help about User Manager for more information.

How to Set Up and Use VCM Auditing

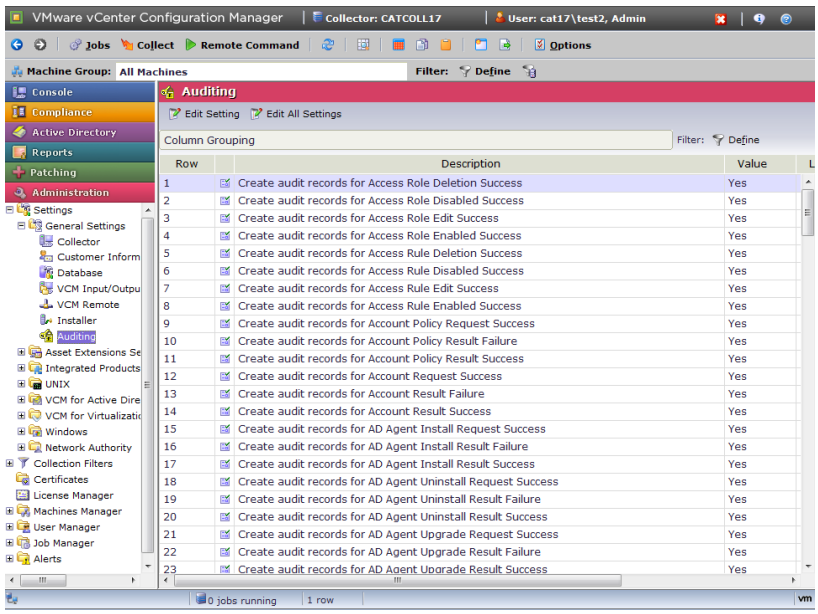
The VCM Auditing capability tracks all changes in the security aspects of VCM. Security-related events are written to the Windows Event Log, which is stored on the Collector, independent of the VCM application. The format of the event log prohibits any modifications to the recorded entries, making it a secure, tamper-proof auditing record of changes in security.

When a user performs an action in VCM that affects security, and the auditing setting that corresponds to that change is enabled, the event is written to the event log. Examples of VCM user actions that cause events to be written to the event log include user logon/logoff, session timeouts, changes in managing users, changes to passwords and administration settings, changes in network accounts and authority, collection requests, and service and registry changes.

NOTE Auditing settings can be enabled or disabled only by users who are assigned and logged in with the Admin role.

---

1. To view the VCM Auditing settings, navigate to the **Administration** slider. Select **Settings** | **General Settings** | **Auditing**.
2. To change an auditing setting, highlight a setting and then click **Edit Setting**. When a user changes an auditing setting, the VCM Auditing data grid displays the user's name in the Last Modified By column.


VMware vCenter Configuration Manager
Collector: CATCOLL17
User: cat17\test2, Admin
Jobs
Collect
Remote Command
Options
Machine Group: All Machines
Filter: Define
Console
Compliance
Active Directory
Reports
Patching
Administration
Settings
General Settings
Collector
Customer Inform
Database
VCM Input/Outpu
VCM Remote
Installer
Auditing
Asset Extensions Se
Integrated Products
UNIX
VCM for Active Dire
VCM for Virtualizatic
Windows
Network Authority
Collection Filters
Certificates
License Manager
Machines Manager
User Manager
Job Manager
Alerts
Auditing
Edit Setting
Edit All Settings
Column Grouping
Filter: Define
Row
Description
Value
1 Create audit records for Access Role Deletion Success Yes
2 Create audit records for Access Role Disabled Success Yes
3 Create audit records for Access Role Edit Success Yes
4 Create audit records for Access Role Enabled Success Yes
5 Create audit records for Access Rule Deletion Success Yes
6 Create audit records for Access Rule Disabled Success Yes
7 Create audit records for Access Rule Edit Success Yes
8 Create audit records for Access Rule Enabled Success Yes
9 Create audit records for Account Policy Request Success Yes
10 Create audit records for Account Policy Result Failure Yes
11 Create audit records for Account Policy Result Success Yes
12 Create audit records for Account Request Success Yes
13 Create audit records for Account Result Failure Yes
14 Create audit records for Account Result Success Yes
15 Create audit records for AD Agent Install Request Success Yes
16 Create audit records for AD Agent Install Result Failure Yes
17 Create audit records for AD Agent Install Result Success Yes
18 Create audit records for AD Agent Uninstall Request Success Yes
19 Create audit records for AD Agent Uninstall Result Failure Yes
20 Create audit records for AD Agent Uninstall Result Success Yes
21 Create audit records for AD Agent Upgrade Request Success Yes
22 Create audit records for AD Agent Upgrade Result Failure Yes
23 Create audit records for AD Agent Upgrade Result Success Yes
0 jobs running
1 row

For details about the Auditing settings, and viewing the Windows Event Log, see the Administration: Auditing Settings topic in the online Help.

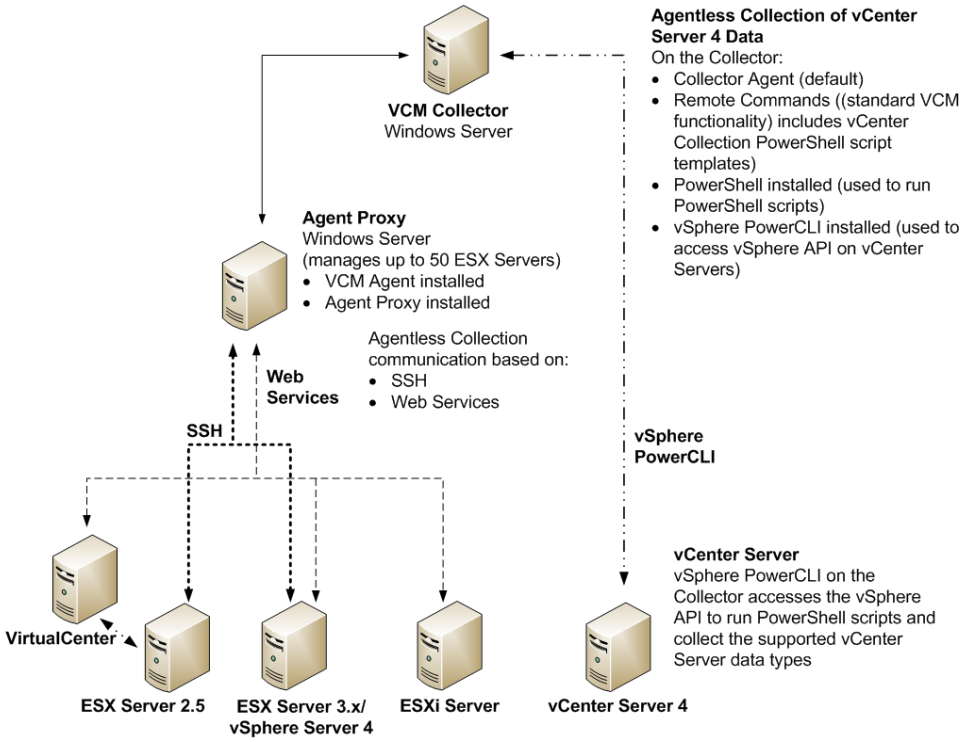
Getting Started with VCM for Virtualization

6

VCM collects virtualization configurations for Virtual Machine (VM) Host servers and their respective VMs (also known as Guests) through a single console. In addition, it collects operating system and security information for VM Host servers. Virtual machine data is displayed in the Console slider under the Virtual Environments node, providing a logical grouping of the configurations of VM Host servers and VM Guests. This grouping allows you to view your Virtual Environments at an enterprise level, and to drill into the specific details. Additionally, VCM correlates virtualization data for VM Guests with their operating system and security data from standard VCM, thus providing a holistic view of your enterprise.

Virtual Environment Configuration

VCM uses VCM-based communication channels in the form of a Remote Client Proxy to collect data from VMware ESX/ESXi/vSphere Servers and VirtualCenter/vCenter Servers.


VCM Collector
Windows Server
Agentless Collection of vCenter Server 4 Data
On the Collector:
• Collector Agent (default)
• Remote Commands ((standard VCM functionality) includes vCenter Collection PowerShell script templates)
• PowerShell installed (used to run PowerShell scripts)
• vSphere PowerCLI installed (used to access vSphere API on vCenter Servers)
Agent Proxy
Windows Server
(manages up to 50 ESX Servers)
• VCM Agent installed
• Agent Proxy installed
Agentless Collection communication based on:
• SSH
• Web Services
Web Services
SSH
vSphere PowerCLI
vCenter Server
vSphere PowerCLI on the Collector accesses the vSphere API to run PowerShell scripts and collect the supported vCenter Server data types
VirtualCenter
ESX Server 2.5
ESX Server 3.x/ vSphere Server 4
ESXi Server
vCenter Server 4

The VCM Agent is not installed directly on the ESX/vSphere Servers and vCenter Servers; instead collections are accomplished using what is referred to as "agentless collections". There are two types of agentless collections, and each type is specific to a particular configuration. One type uses an Agent Proxy, and the other type uses a direct call to the vSphere API using vSphere PowerCLI.

The collected data is displayed in the **Console | Virtual Environments**.

ESX 2.5/3.x,vSphere 4, and ESXi Servers Collections

When collecting from ESX 2.5/3.x, vSphere 4, and ESXi Servers, you must configure at least one VCM Agent Proxy machine. The Collector communicates with the Agent Proxy, and the Agent Proxy then directly communicates with the ESX 2.5/3.x, vSphere 4, and ESXi Servers using SSH and/or Web Services for necessary data collection actions. In the case of ESX 2.5, the Agent Proxy communicates with the VirtualCenter Servers to collect certain ESX 2.5 data it cannot collect directly. The data is processed by the Agent Proxy and relayed to the Collector.

The Agent Proxy machine must be a Windows server that meets the minimum hardware and software requirements specified in the *VCM Hardware and Software Requirements Guide*. A single Agent Proxy machine supports up to 50 ESX/ESXi/vSphere Servers.

VCM Support of ESXi

VCM supports collecting Guests and Hosts data from ESXi machines. ESXi does not support SSH, and therefore UNIX/Linux data classes data cannot be collected. Only Web Service Settings are required for ESXi machines.

IMPORTANT When collecting from ESXi, attempting to collect any data other than VM Hosts or VM Guests data from the ESXi machine will result in a collection failure. This includes collection filters supplied with the product and targeted for ESX 2.5 and ESX 3.x/vSphere 4. Running such collections on all the All VM Hosts Machine will also fail for ESXi machines.

Only the VM Hosts and VM Guests data types are available for collection, and it is not possible to run UNIX Remote Commands. You may see SSH settings in the License VM Host wizard for the ESXi machine, but you do not need to configure them.

vCenter Server Collections

When collecting from vCenter Server, you must configure the Collector with the necessary components, including an Agent (installed by default), Remote Commands (VCM functionality that includes vCenter Collection PowerShell templates to be the model for your local scripts), PowerShell 2.0, and vSphere PowerCLI 2.0. The Collector Agent runs the vCenter Collection remote commands, which include your Powershell scripts, and then vSphere PowerCLI accesses the vSphere API on the vCenter Servers to perform the necessary data collection actions. The data is relayed to the Collector and added to the database.

When collecting using the vCenter collection remote command, neither SSH nor Web Services should be configured when using this collection method. For configuration information, see "Configuring vCenter Server Data Collections" on page 137.

Configuring Agent Proxy Virtualization Collections

The following table provides a list of installation and configuration procedures to follow when configuring VCM.

IMPORTANT The steps must be executed in the order presented.

In order to configure VCM to seamlessly collect from virtual machines, the various actions specified in the following sections are performed on three machines. The action locations are as follows:

- **In VCM:** The action is performed using the VCM Portal.
- **On Agent Proxy machine:** The action is performed on the Windows machine designated as the Agent Proxy.
- **On ESX/vSphere Server:** The action is performed on the ESX/vSphere Server.

Configuration Section	VCM	Agent Proxy Machine	ESX/vSphere Server
Configuring Agent Proxy Machines	Step 1: Licensing Agent Proxy Machines		
	Step 2: Installing the Agent on the Agent Proxy Machines		
	Step 3: Performing Collections Using the Machines Data Type		
	Step 4: Installing Agent Proxies		
Configuring ESX Servers			Step 5: Copying Files from the Collector to the ESX Servers **
			Step 6: Running Scripts on the ESX Server **
	Step 7: Adding ESX Servers to VCM		
	Step 8: Licensing the ESX Server in VCM		
	Step 9: Licensing ESX Server Machines as Virtual Machine (VM) Hosts		
Configuring Web Services for ESX Server Communication			Step 10: Adding the Web Services User to the Administrator Role Using the VI Client **

Configuration Section	VCM	Agent Proxy Machine	ESX/vSphere Server
		Step 11: Installing the ESX Web Services Certificate the Agent Proxy Machines **	
			Step 12: *For ESX 2.5.x Only*: Setting Up VirtualCenter to Collect Virtualization Data
	Step 13: Adding Web Services Settings		
Performing Initial Collection	Step 14: Performing an Initial Virtualization Collection		
Exploring Collection Results	Step 15: Exploring Virtualization Collection Results		

NOTE ** A Deployment Tool is available from VMware Customer Support to assist you with this process for ESX 3.x/vSphere 4and ESXi. To use the tool, contact VMware Customer Support; otherwise, follow the steps in the following sections.

Configuring Agent Proxy Machines

The Agent Proxy machine is a Windows machine configured to communicate with ESX/vSphere Servers and to remotely collect data from those servers. Using a separate Windows machines as your Agent Proxy is the most effective way to manage the virtualization environments. The recommendation to use a separate Windows machine is in recognition that the Collector already performs a consistently high level of work. Moving Agent Proxy activity to the separate machine optimizes performance.

NOTE The Agent Proxy should not be installed on an Active Directory Domain Controller.

The configuration of an Agent Proxy machine includes of the following steps:

1. Licensing the Agent Proxy machine.
2. Installing the Agent on the Agent Proxy machine.
3. Performing a Collection on the Agent Proxy machine.
4. Installing the Agent Proxy files.

All the actions in this section are performed in VCM.

Licensing Agent Proxy Machines

Use the following procedure to license the Windows machine designated as your Agent Proxy.

In VCM:

1. Click **Administration | Machines Manager | Available Machines | Available Windows Machines**.
2. In the data grid, select your designated Agent Proxy machine, and then click **License**. The **Machines** page of the Available Machines License wizard appears.
3. Confirm that your machine appears in the **Selected** list, and then click **Next**. The **Product License Details** page appears.
4. A list of your total and available licenses is displayed. Confirm that a Windows license is consumed, and then click **Next**.
5. Confirm your action, and then click **Finish**.

NOTE If your Agent Proxy machine is not displayed in the list of **Available Windows Machines**, it may already be licensed. To determine if it is licensed in VCM, click **Administration | Machine Manager | Licensed Machines| Licensed Windows Machines**. If it is not listed, see Discover, License, and Install Windows Machines for information on how to add it to VCM.

Installing the Agent on the Agent Proxy Machine

After a machine is licensed, the VCM Agent must be installed. The Agent is required in order to perform a collection from the machine.

In VCM:

1. Click **Administration | Machines Manager | Licensed Machines | Licensed Windows Machines**.
2. In the data grid, select your Agent Proxy machine, and then click **Install**. The **Machines** page of the **Install Product** wizard appears.
3. Confirm that your machine appears in the **Selected** list, and then click **Next**. The **Install Options** page appears.
4. In the **Install At** area, type the **Share** and **Path** if they are different from the default values.
5. In the **Install from** area, select the Collector you are using to manage this machine and the virtual machines.
6. In the **Options** area, select your communication method. If you are re-tasking a machine as your Agent Proxy, select **Reinstall Agent**.
7. Click **Next**. The **Schedule** page appears.
8. Select **Run Action now** to immediately install the Agent. Select **Schedule the Action to run later** and configure the time and date to install the Agent at a later time.
9. Click **Next**. The **Important** page appears. Review the contents, click **Back** to make any changes, and then click **Finish**.

Performing a Collection Using the Machines Data Type

Before you can add a machine as an Agent Proxy, you must Collect from the machine using the Machines data type. This process verifies that the Agent Proxy machine meets the minimum requirements to serve as an Agent Proxy machine.

In VCM:

1. Click **Collect**. The **Collection Type Selection** dialog box appears.
2. Select **Machine Data**, and then click **OK**.
3. In the **Available** list, double-click the designated Agent Proxy machine to move it to the **Selected** list.
4. Select the **Select Data Types to collect from these machines** option, and then click **Next**.
5. Expand the **Windows** node, and then select the **Machines** data type check box.
6. Select the **Use default filter** option, and then click **Next**.
7. Click **Finish**.
8. Before proceeding to the next set of steps, verify that you have successfully collected the Machines data type. Click **Console | Windows (tab) | Operating System | Machines**, then verify that your Agent Proxy machine appears in the data grid. If you have recently upgraded the agent to VCM 5.3, please ensure that you re-collect the machines data as noted above.

Installing Agent Proxies

Installing the Agent Proxy adds the SSH key and the CSI_COMM_Proxy_SVC group to the target machine, and adds the SSH key pairs to the database.

IMPORTANT Some platforms are no longer supported for the current Agent Proxy version. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and Agent Proxy versions.

In VCM:

1. Click **Administration | Machines Manager | Additional Products | vCenter CM for Virtualization | Agent Proxies**.
2. Select the machine or machines on which you are installing the Agent Proxy. If your designated Agent Proxy machine is not displayed, it failed to meet one or more of the following requirements:
   - The machine is running Windows Server 2003 Service Pack 2 or later.
   - The machine is licensed in VCM.
   - The 4.11 Agent or later is installed.

   Resolve the issue and continue.
3. Click **Install**. The **Machines** page of the **Install Agent Proxies** wizard appears.
4. The available machines are displayed in the upper list. The selected machines are displayed in the lower list. You can perform the following actions on the page:
   - **All Machines:** Select the option to install the Agent Proxy on all eligible machines.
   - **Selected Machines Only:** (Default option) Select the option to install the Agent Proxy on all machines listed in the lower pane.
   - **Filtered Machines:** Click **Define** to create a filter based on Machine Name or Domain Name, and then select the **Filtered Machines** option.
   - **Arrow buttons:** Select a machine name in one of the panes and use the arrow buttons to move it from one pane to the other. Additionally, you may double-click a machine name to move it between panes.
5. Click **Next**. The **Option** page appears.

6. Configure the following options:
   - **Install From:** In the drop-down list, select the name of the Collector used to manage virtual machines.
   - **Schedule:** Select **Run Action now** to install immediately, or select **Schedule the Action to run later** and configure the settings to correspond to you company policies.
7. Click **Next**. The **Important** page appears. Review the contents, click **Back** to make any necessary alterations.
8. Click **Finish**. The Agent Proxy is installed at the time specified.
9. Verify that all jobs have completed successfully before proceeding to the next step. To do so, click **Jobs**, located on the Portal toolbar, to view the Jobs Summary. You can also verify jobs for the past 24 hours if you think that you may have missed it. Go to **Administration | Job Manager | History | Other Jobs | Past 24 Hours**.

Advanced information

When the installation process is completed on an Agent Proxy machine, you can see the following results:

On the Agent Proxy machine:

- Added the CSI_COMM_Proxy_SVC group, with a local user.

  NOTE If you need to replace a local user in the CSI_COMM_Proxy_SVC group with a new local user, the new account must have full control of `[drive]:\Program Files\VMware\VCM` and have full control of the Configuresoft registry key (`HKEY_LOCAL-MACHINE\Software\Configuresoft`).

  If keys have already been generated, the `agentdata\protected` folder must be deleted and new keys generated/uploaded and distributed.

  To change the password for the new user account, you must log in as the user rather than allowing an administrator to reset the password. If the password is changed by the new user, the keys do not need to be regenerated.

- Copied the `<agent_proxy_machine_name>_ssh_public_key.txt` to `[drive]:\Windows\CMAgent\<agent_proxy_machine_name>_ssh_public_key.txt`

On the Collector:

- Installed the Agent Proxy. See the **Agent Proxies** data grid, **Agent Proxy Version** column.
- Added the keys to the database. See the **Agent Proxies** data grid, **Key Available in DB** column.

If you are configuring your Collector as your Agent Proxy, see "Configuring a Collector as an Agent Proxy" on page 265 for a different set of procedures. After completing the steps, continue with "Configuring ESX/vSphere Servers" on page 123.

Configuring ESX/vSphere Servers

After configuring the Agent Proxy machines, you are now ready to configure the ESX/vSphere Servers. The process used to configure the ESX/vSphere Servers requires copying files to the ESX/vSphere Servers and performing configuration tasks in VCM.

The tasks include the following:

1. Copying files from the Collector to the ESX/vSphere Server (requires access to the Collector and to the target ESX/vSphere Servers).
2. Running script files on the ESX/vSphere Server (requires access to the ESX/vSphere Servers).
3. Adding ESX/vSphere Servers to VCM.
4. Licensing the ESX Servers in VCM.
5. Licensing ESX machines as Virtual Machine (VM) Hosts.

The actions in this section are performed on the Collector, on the ESX/vSphere Servers, and in VCM.

Copying Files to the ESX/vSphere Server

Use your preferred method (such as Secure Copy Protocol (SCP) or FTP) to copy the following files from your Collector and Agent Proxy machine to your ESX/vSphere Server in Service Console Operating System under the `/tmp` directory (for example).

NOTE A Deployment Tool is available from VMware Customer Support to assist you with the following process for ESX 3.x/vSphere 4 and ESXi. To use the tool, contact VMware Customer Support; otherwise, follow the steps in the following procedure.

On the Collector and Agent Proxy, and on the ESX/vSphere Servers:

1. Copy the following files:

   Located on the Agent Proxy:

   ```
   [drive:]\Program Files\VMware\VCM\Tools\Virtualization\<machine>_ssh_public_key.txt
   ```

   Located on the Collector:

   ```
   [drive:]\Program Files\VMware\VCM\Tools\Virtualization\csiprep.py
   ```

   ```
   [drive:]\Program Files\VMware\VCM\Tools\Virtualization\csiprep.config
   ```

2. On the ESX/vSphere Servers, add the files in Service Console Operating System. For example, add the files to the `/tmp` directory.

Running Scripts on the ESX/vSphere Server

NOTE A Deployment Tool is available from VMware Customer Support to assist you with the following process for ESX 3.x/vSphere 4 and ESXi. To use the tool, contact VMware Customer Support; otherwise, follow the steps in the following procedure.

On the ESX/vSphere Servers:

1. Log on to the ESX/vSphere Server Service Console Operating System as **root**.
2. Go to the directory location where you copied the files from the Collector.
3. Modify the `csiprep.config` file as follows:
   - Set the CSI_USER variable to the name of the connection account (new or existing). This is the account that will be used for SSH collections. Example: CSI_USER = csi_acct
   - Set the path to the public_key file for the CSI_PUBKEY variable. Example: CSI_PUBKEY=/<path to the public key file>/<machine>_ssh_public_ key.txt

Setting these variables will enable the execution script listed in Step 4 (**csiprep.py**) to create a user account on the ESX/vSphere Server (if it does not already exist), add that user to the **sudoer** file, and then add the key for that user to the authorized key file. If the user account does not currently exist, then the **csiprep.py** script creates it with the following settings:

- username = CSI_USER
- group name = User name
- uid = Next user ID available in /etc/passwd (Example: If the last one used is 506, then the next user would be 507.)
- password = None set (An Administrator must set the password. This account can also be used for Web Services communication.)
- home directory = /home/<new_user>/.ssh/authorized_keys
- shell = :/bin/bash

4. You must be **root** to run the prep script. Additionally, you must also have the **root** password or existing sudo access, as an account may be created and the sudo config file is modified. The `/etc/sudoers` configuration file is modified to grant root access for the CSI_USER account, which enables VCM to collect information that requires root access from the ESX Service Console Operating System. If you have a root access password, execute the following in the command prompt:

   ```
   su –
   cd <directory location of files copied>
   python csiprep.py
   ```

   If you have sudo access with your current account, execute the following in the command prompt:

   ```
   sudo python csiprep.py
   ```

   The ESX/vSphere Server should now have a new/modified account for CSI_USER, full sudo settings, and the public key stored in the /home/$CSI_USER/.ssh/authorized_keys. The CSI_USER variable can be an existing account (in which case the account will have any missing elements set up, such as sudo or .ssh).

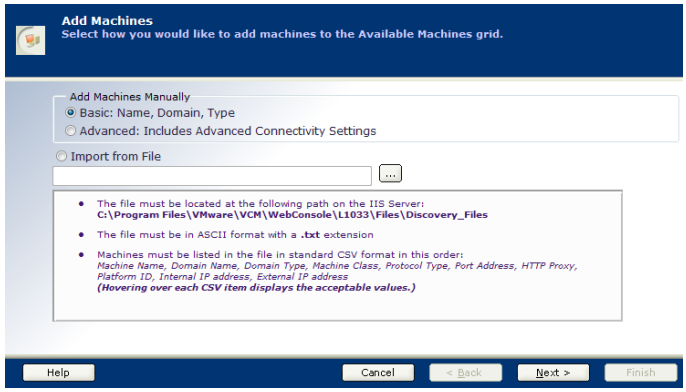
5. Once you complete this step, a log file is generated (`csiprep.log`). At this point you may remove the files. It is recommended that you keep the .log file for troubleshooting purposes.

Adding ESX/vSphere Servers to VCM

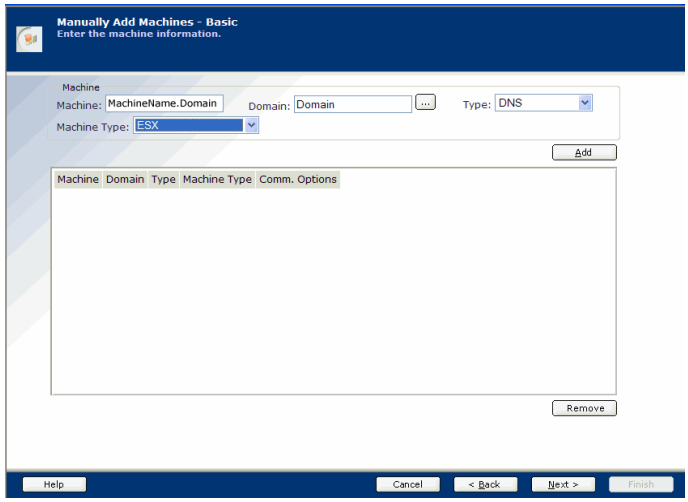
Use the following procedure to manually add your ESX/vSphere Server into VCM's list of Available Machines if they were not included in a discovery.

In VCM:

1. Click **Administration** | **Machines Manager** | **Available Machines** | **Available UNIX Machines**.
2. Click **Add Machines**. The **Add Machines** page of the **Discovery Manual Machine Entry** wizard appears.


Add Machines
Select how you would like to add machines to the Available Machines grid.
Add Machines Manually
Basic: Name, Domain, Type
Advanced: Includes Advanced Connectivity Settings
Import from File
The file must be located at the following path on the IIS Server:
C:\Program Files\VMware\VCM\WebConsole\L1033\Files\Discovery_Files
The file must be in ASCII format with a .txt extension
Machines must be listed in the file in standard CSV format in this order:
Machine Name, Domain Name, Domain Type, Machine Class, Protocol Type, Port Address, HTTP Proxy, Platform ID, Internal IP address, External IP address
(Hovering over each CSV item displays the acceptable values.)
Help
Cancel
< Back
Next >
Finish

3. Select **Basic Name, Domain, Type**, and then click **Next**. The **Manually Add Machines - Basic** page appears.



4. Type your ESX/vSphere Server **Machine** using a fully qualified domain name (FQDN), select the **Domain**, and select DNS as the **Type**. In the **Machine Type** drop-down list, select ESX.

NOTE Enter the fully qualified machine name of the ESX/vSphere Server as the "Machine Name". The ESX server machine name must match the machine's Host Identification name, including the domain, as displayed in the vSphere/Virtual Infrastructure Client's Configuration tab | DNS and Routing section. The name on the ESX Web Server certificate must also match the FQDN of the host machine.

5. Click **Add**.
6. Click **Next**.
7. Confirm your addition, and then click **Finish**.

NOTE For more information on other options for adding Machines (such as an import file or a discovery rule), refer to the online Help.

Licensing the ESX/vSphere Server in VCM

Licensing the ESX Server uses a UNIX/Linux/Mac Server license.

In VCM:

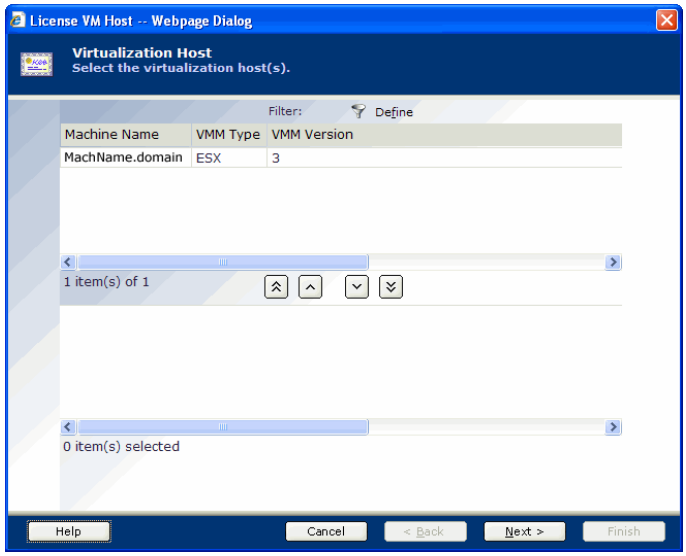
1. Click **Administration** | **Machines Manager** | **Available Machines** | **Available UNIX Machines**.
2. Select your ESX/vSphere Server in the data grid, and then click **License**.
3. Confirm that your machine appears in the **Selected** list, and then click **Next**.
4. A list of your total and available licenses appears. Confirm that a UNIX Linux/Mac Server license is consumed, and then click **Next**.
5. Confirm your action, and then click **Finish**.

Licensing ESX/vSphere Server Machines as Virtual Machine (VM) Hosts

Licensing a VM Host uses a Virtualization license.

In VCM:

1. Click **Administration** | **Machines Manager** | **Additional Components** | **VCM for Virtualization** | **Licensed VM Hosts**.
2. Click **License**. The **Virtualization Host** page of the **License VM Host** wizard appears.

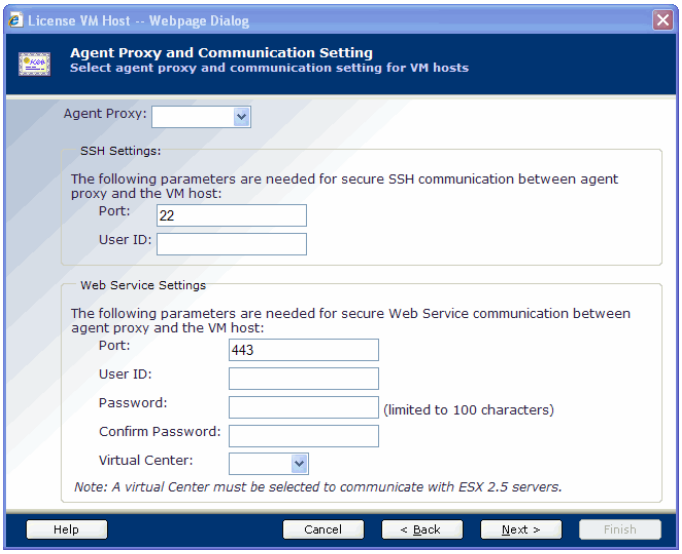


3. The upper pane displays the available machines. The lower pane displays the machines to be licensed. Double-click the machines in the upper pane to add it to the list in the lower pane. Click **Next**. The licensing details page appears.

NOTE If no machines are listed in this data grid to be licensed, return to Licensing the ESX/vSphere Server to verify that you have licensed your ESX machines with UNIX/Linux licenses.

---

4. Review the licenses. Each ESX/vSphere Server consumes one UNIX/Linux server license and one Virtualization license; however, you are charged only one license fee for each ESX/vSphere Server, and both licenses are included. Click **Next.** The **Agent Proxy and Communication Setting** page appears.


License VM Host -- Webpage Dialog
Agent Proxy and Communication Setting
Select agent proxy and communication setting for VM hosts
Agent Proxy:
SSH Settings:
The following parameters are needed for secure SSH communication between agent proxy and the VM host:
Port:
22
User ID:
Web Service Settings
The following parameters are needed for secure Web Service communication between agent proxy and the VM host:
Port:
443
User ID:
Password:
(limited to 100 characters)
Confirm Password:
Virtual Center:
Note: A virtual Center must be selected to communicate with ESX 2.5 servers.
Help
Cancel
< Back
Next >
Finish

5. Enter information related only to the following areas:
   - **Agent Proxy**: Select the configured Agent Proxy machine.
   - **SSH Settings**: Specify the port and user ID used in the SSH file on the ESX server. The User ID is the same account as the connection account specified in Running Scripts on the ESX/vSphere Server.

   NOTE Even if you have this information, do not configure the Web Services settings in this wizard. Web Services configuration is presented in Configuring Web Services for ESX/vSphere Server Communication. For information about these fields and their values, click Help at any time when working in this wizard.
6. When the settings are configured, click **Next**.
7. Confirm your change, and then click **Finish**.
8. A pop-up window asks if you want to perform an instant collection. Click **OK** to run a **Machines - General** collection on the ESX/vSphere Servers.
9. Confirm that **Machines - General** data was collected by navigating to **Console | UNIX | Operating Systems | Machines | General**. Review the data grid and note the versions of your ESX/vSphere Servers.

Configuring Web Services for ESX/vSphere Server Communication

The Web Services communication must be set up to allow collections of Virtual Environments VM Host and VM Guest data types. The Web Service interface exists on ESX 3.x/vSphere 4, and ESXi servers only. To collect this data on ESX 2.5.x servers, you must have VirtualCenter 2.0.x managing your ESX 2.5.x servers. If you want to collect from an ESX 2.5 Server, perform the following procedure on the VirtualCenter Server that manages your ESX/vSphere Server.

NOTE Although Web Services Settings are optional when first licensing ESX, they impact the types of collections that you can perform against ESX/vSphere Servers.

Use the following procedures to configure Web Services:

1. Adding the Web Services User to the Administrator Role Using the VI Client/vCenter Client.
2. Installing the ESX Web Service Certificate on the Agent Proxy Machine.
3. For ESX 2.5 Only: Setting Up VirtualCenter to Collect Virtualization Data.
4. Adding Web Services Settings to VCM.

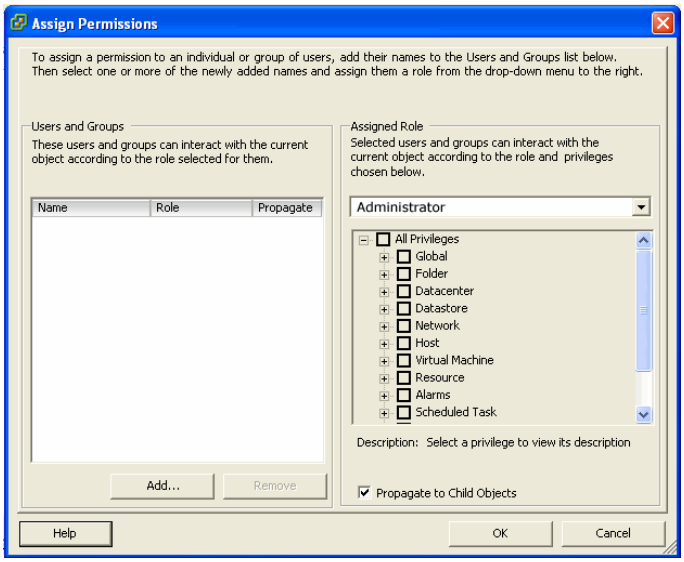
Adding the Web Services User to the Administrator Role Using the VI Client/vCenter Client

The following procedure uses the Virtual Infrastructure (VI) Client/vCenter Client to add the Web Services user to the Administrator role. For ESX 3.x/vSphere 4, and ESXi, you can use the same account that you created in Running Scripts on the ESX/vSphere Server (CSI_USER). For ESX 2.5, you must use a Windows account to access the Web Services interface on the VirtualCenter machine.

NOTE A Deployment Tool is available from VMware Customer Support to assist you with the following process for ESX 3.x/vSphere 4 and ESXi. To use the tool, contact VMware Customer Support; otherwise, follow the steps in the following procedure.

On the ESX/vSphere Server:

1. Start the VI Client/vCenter Client.
2. Log in as one of the following users:
   - For ESX 3.x/vSphere 4, and ESXi, login to the ESX/vSphere Server as **root**. For ESX 3.x/vSphere 4 and ESXi, you must log on directly to the ESX/vSphere Server and not the VirtualCenter Server to add the necessary permission.
   - For ESX 2.5, log on to the VirtualCenter Server as a Domain or Local Administrator.
3. Select the ESX/vSphere Server. Click **Inventory** | **Host** | **Add Permission**. The **Assign Permissions** dialog box appears.


Assign Permissions
To assign a permission to an individual or group of users, add their names to the Users and Groups list below.
Then select one or more of the newly added names and assign them a role from the drop-down menu to the right.
Users and Groups
These users and groups can interact with the current object according to the role selected for them.
Name
Role
Propagate
Add...
Remove
Assigned Role
Selected users and groups can interact with the current object according to the role and privileges chosen below.
Administrator
All Privileges
Global
Folder
Datacenter
Datastore
Network
Host
Virtual Machine
Resource
Alarms
Scheduled Task
Description: Select a privilege to view its description
Propagate to Child Objects
Help
OK
Cancel

4. Click **Add**.
5. Select the user name that you defined in Running Scripts on the ESX/vSphere Server (csi_acct in that example). For ESX 2.5, select the Windows account you want to use for Web Services communication. Click **Add**. The user name is added to the **Users and Groups** list.

   NOTE Although the example uses the same user account for both Web Services and SSH, they are not required to be the same account.

6. In the **Assigned Roles** drop-down list, select **Administrator**.
7. Click **OK**.
8. To confirm your change, click the **Admin** tab, then select **Administrator** as the role. The user name should appear underneath the **ha-folder-root** directory and ESX/vSphere Server.

   NOTE If you do not want to add the user to the Administrator role, contact VMware Customer Support for details about defining a different role.

Installing the ESX Web Services Certificate on the Agent Proxy Machine

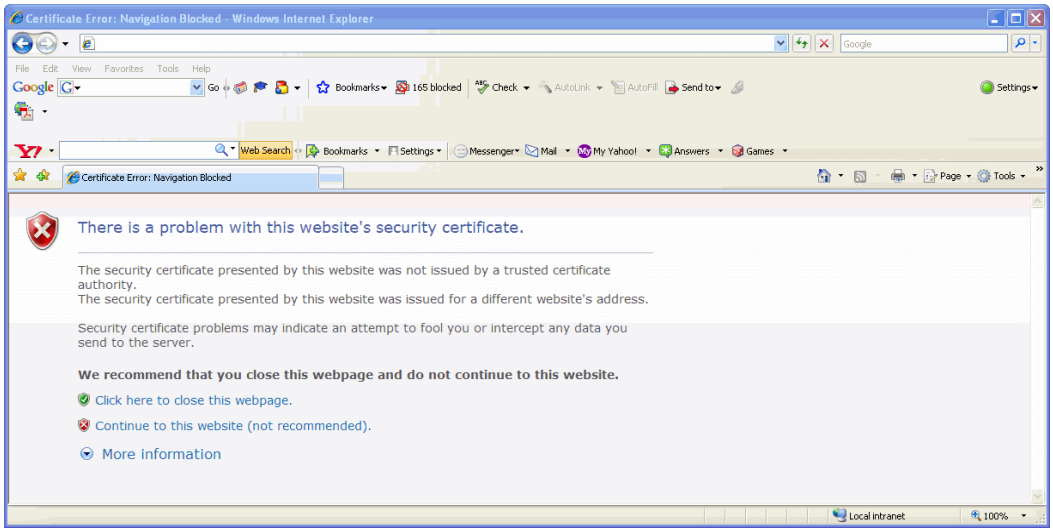
You must be logged into the Agent Proxy machine to perform this step. ESX and VirtualCenter come out-of-the-box with a self-signed certificate. If you are using this certificate, use the following procedure to install the ESX/vSphere Server or VirtualCenter (for ESX 2.5 only) Web Service Certificate on the Agent Proxy machine. You must use a pre-trusted certificate to collect data from the Virtual Infrastructure (VI) Web Services interface. As stated above, to collect from ESX 2.5 Servers, VCM collects data for those ESX 2.5 Servers from VirtualCenter 2.0. However, the VirtualCenter 2.0 out-of-the-box, self-signed certificate is invalid and will not work, even if it has been pre-trusted. In this case, you need to install a valid certificate in order to collect. If you have a Public Key Infrastructure (PKI) in place or already trust your ESX or VirtualCenter Server machine's certificate by other means, this step is not necessary. For more information on VMware's recommendations on certificate management, refer to VMware's technical note about replacing certificates, located online at: http://www.vmware.com/pdf/vi_vcserver_certificates.pdf.

VMware assumes that you are using https for Web Services communication for VI Client/vCenter Client and VirtualCenter/vCenter Server. If you are using http instead, call VMware Customer Support for assistance. By default, collections will fail if a certificate error exists. If the certificate fails, a security error message appears. For assistance, call VMware Customer Support.

NOTE A Deployment Tool is available from VMware Customer Support to assist you with the following process for ESX 3.x/vSphere 4 and ESXi. To use the tool, contact VMware Customer Support; otherwise, follow the steps in the following procedure.

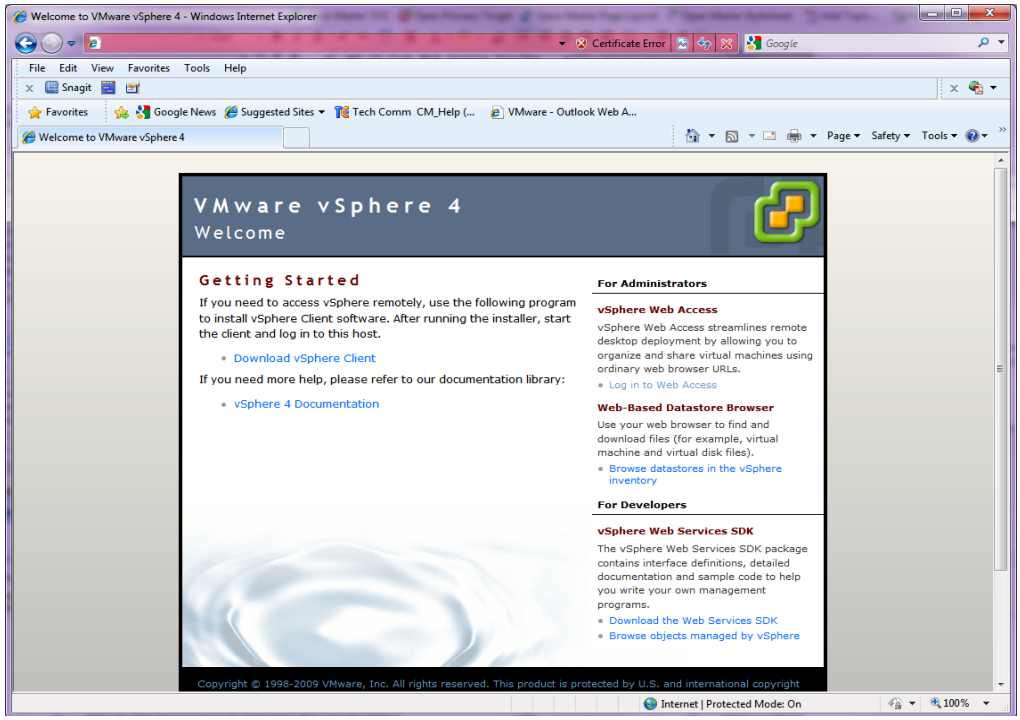
On the Agent Proxy machine:

1. Log on to the Agent Proxy machine. The steps provided here cannot be performed remotely.
2. Open Internet Explorer, and then navigate to the location of your ESX or VirtualCenter machine (for ESX 2.5 only).
   For example, `https://<ESXhost/vSpherehost>` or `https://<VirtualCenterhost/vCenterhost box>`:
   Internet Explorer displays an error message, indicating a problem with the security certificate.

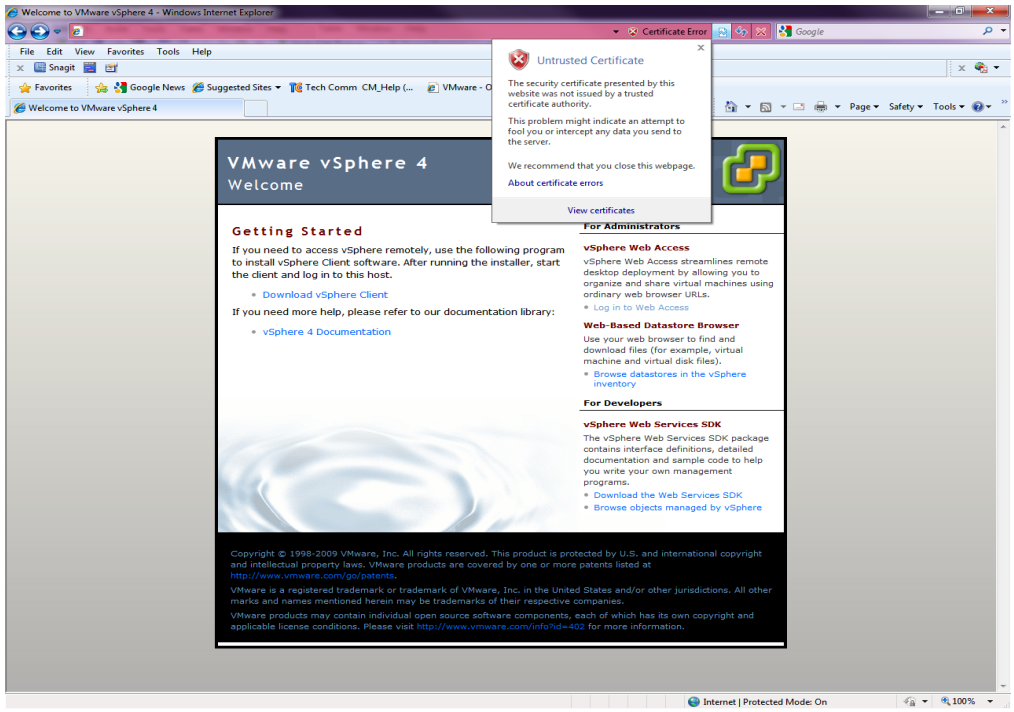

Certificate Error: Navigation Blocked - Windows Internet Explorer
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
Local intranet
100%

NOTE For older versions of Internet Explorer these steps may vary. Ensure you install the certificate as described below.

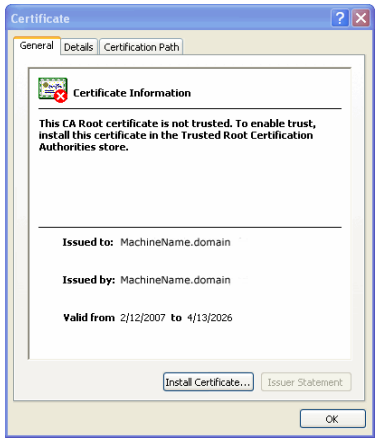
3. Click **Continue to this website**. The browser displays the **Welcome** page.


Welcome to VMware vSphere 4 - Windows Internet Explorer
Certificate Error
VMware vSphere 4
Welcome
Getting Started
If you need to access vSphere remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Download vSphere Client
If you need more help, please refer to our documentation library:
vSphere 4 Documentation
For Administrators
vSphere Web Access
vSphere Web Access streamlines remote desktop deployment by allowing you to organize and share virtual machines using ordinary web browser URLs.
Log in to Web Access
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in the vSphere inventory
For Developers
vSphere Web Services SDK
The vSphere Web Services SDK package contains interface definitions, detailed documentation and sample code to help you write your own management programs.
Download the Web Services SDK
Browse objects managed by vSphere
Copyright © 1998-2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright
Internet | Protected Mode: On
100%

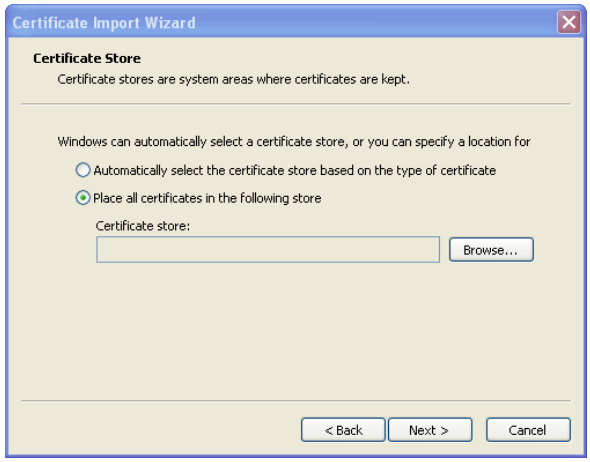
4. Click the **Certificate Error** field on the red-shaded address bar. A dialog box appears with information about the error message.


Untrusted Certificate
The security certificate presented by this website was not issued by a trusted certificate authority.
This problem might indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage.
About certificate errors
View certificates
VMware vSphere 4
Welcome
Getting Started
If you need to access vSphere remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Download vSphere Client
If you need more help, please refer to our documentation library:
vSphere 4 Documentation
For Administrators
vSphere Web Access
vSphere Web Access streamlines remote desktop deployment by allowing you to organize and share virtual machines using ordinary web browser URLs.
Log in to Web Access
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in the vSphere inventory
For Developers
vSphere Web Services SDK
The vSphere Web Services SDK package contains interface definitions, detailed documentation and sample code to help you write your own management programs.
Download the Web Services SDK
Browse objects managed by vSphere
Copyright © 1998-2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.
VMware products may contain individual open source software components, each of which has its own copyright and applicable license conditions. Please visit http://www.vmware.com/info?id=402 for more information.

5. Click **View certificates** at the bottom of this dialog box. The **Certificate** dialog box appears with information about the certificate.



6. Click **Install Certificate**. The **Certificate Import Wizard** appears.


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

7. Click **Place all certificates in the following store**, and then click **Browse**. The **Select Certificate Store** dialog box appears.

8. Click **Show physical stores**. Select **Third-Party Root Certification Authorities** | **Local Computer**. Click **OK**.
9. Click **Next**, and then click **Finish**.

For ESX 2.5.x Only: Setting Up VirtualCenter to Collect Virtualization Data

In VCM:

1. Add your VirtualCenter machine and license it. For more information on how to add and license a Windows machine, see "Licensing Windows Machines" on page 59.
2. Click **Collect** on the Portal toolbar.
3. In the **Available** list, double-click the VirtualCenter machines to add them to the **Selected** list. Select **Select Data Types to collect from these machines**, and then click **Next**.
4. On the **Data Type** dialog box, select **Machines and Services**, and then click **Next**.
5. Click **Finish**.

Adding Web Services Settings

In VCM:

1. Select **Administration** | **Machines Manager** | **Additional Components** | **VCM for Virtualization** | **Licensed VM Hosts**.
2. Click **Change Settings**.
3. Populate the fields displayed in the Web Services box. For information on any of these fields, click **Help** on the wizard page.

NOTE For ESX 2.5 VM Hosts, which collect Web Services data through a VirtualCenter, select the VirtualCenter you configured when setting up in For ESX 2.5.x Only: Setting Up VirtualVirtualCenter Center to Collect Virtualization Data.

Performing an Initial Virtualization Collection

You are ready to perform your collection of Virtual Environments data using the same Collection wizard you have previously used for Windows and UNIX/Linux Collections.

In VCM:

1. Click **Collect** on the Portal toolbar.
2. Select your ESX/vSphere Servers from the **Available** list, clicking the > arrow to move them to the **Selected** list. Click **Select Data Types to collect from these machines**, and then click **Next**. The **Collection Wizard Data Type** dialog box appears.
3. Expand the **UNIX** node, and then select the **Machines - General** data type check box. Expand the **Virtualization** node, and then select the **VM Hosts** and **VM Guests** data types.
4. Click **Use default filters**, and then click **Next**.
5. Click **Finish**.

NOTE If you successfully collect virtualization data, you have correctly configured VCM with a separate Windows machine as your Agent Proxy. This is the recommended configuration. If, however, you want to use your Collector as your Agent Proxy machine, see "Configuring the Collector as an Agent Proxy" in the online Help for detailed precedures. Be aware that this is not the recommended configuration. The Collector already performs a consistently high level of work. Using the same machine for both your Collector and your Agent Proxy may impact Collector performance.

Exploring Virtualization Collection Results

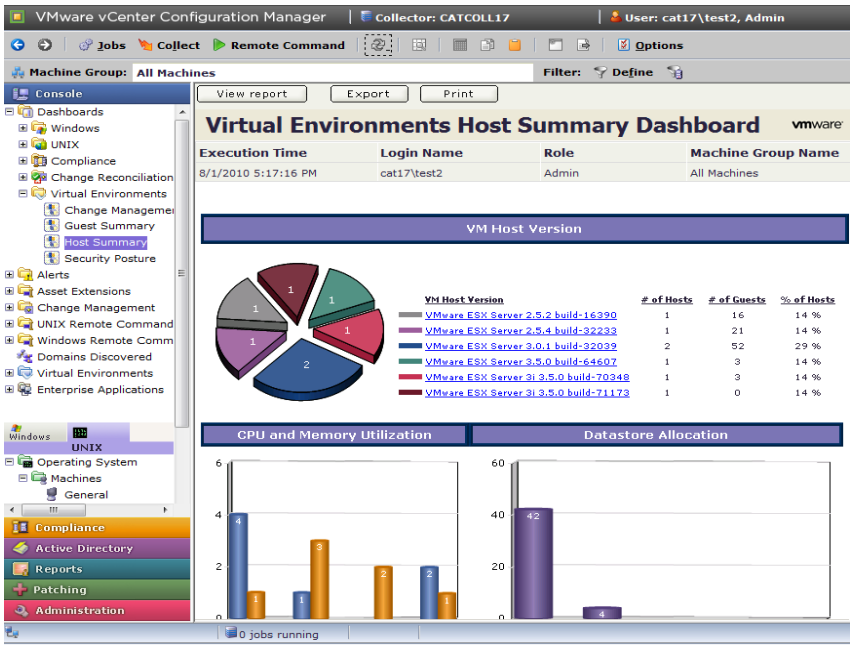
Now that you have performed an initial Virtualization collection, you can explore that data in the Portal. Recall that each Node Summary is run against the current data available in the VCM database. Therefore, Dashboard data is only current as of the time it was collected. In addition, the amount of time it takes for the data to display is based on the volume or complexity of the data requested.

Begin by looking at the UNIX Node Summary located in **Console | UNIX (tab) | Operating System | Machines | General**. From here, you can view a graphical summary of information about your ESX Servers. Click **View data grid** to view more details in a data grid format.

NOTE For the full list of UNIX and Linux data types available for collection on ESX/vSphere Servers refer to the online Help.

Viewing ESX Machine Data

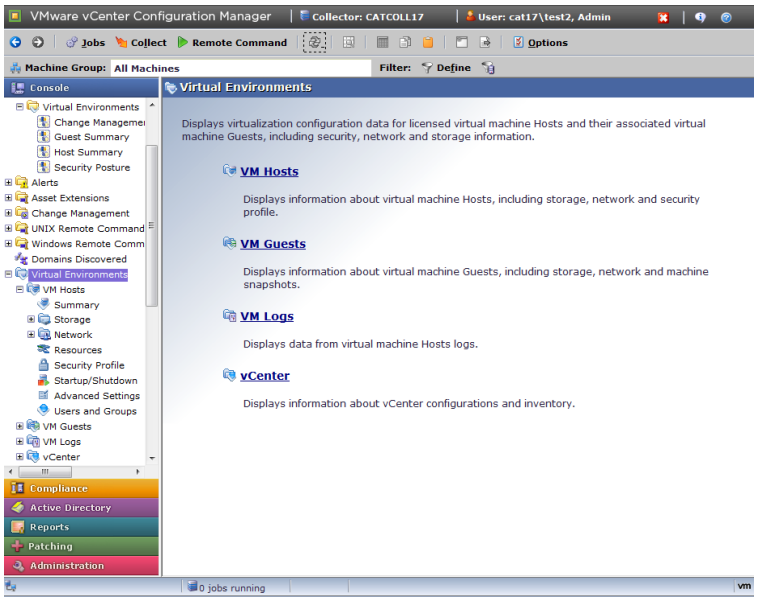
To view your VM Host and Guest Summary, click **Console | Dashboards | Virtual Environments**.



From here, you can view a summary of your VM Guests and Hosts, as well as change management data for your Virtual Environment. Take some time to explore each of these nodes and examine the data available within each node. At any time, click **Help** for more information.

Viewing the Virtualization Environments

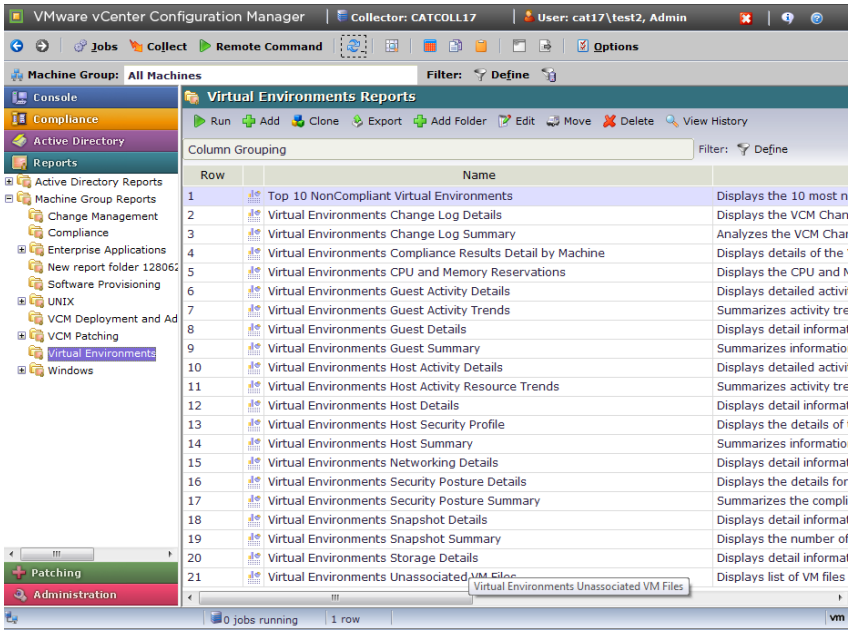
Select **Console** | **Virtual Environments** to begin viewing virtualization configuration data for licensed Virtual Machine Hosts and their associated Virtual Machine Guests, including security, network and storage information.



Several other categories of information (data types) are available under the Virtual Environments node. This is where the remainder of your collected virtualization data is visible through the Portal. Take some time to explore each node, clicking **Help** at any time for more information.

Virtualization Reports

To view reports related to your Virtual Environments, select **Reports** | **Machine Group Reports** | **Virtual Environments**.



Like Dashboards, Reports are run real-time against current data available in the VCM database, therefore the data is only as current as the time that the collections were run. In addition, it may require time for the report to generate, based upon the volume or complexity of the data requested. Additional reports for ESX/vSphere Servers exist under **Reports** | **Machine Group Reports** | **UNIX**, which display information from UNIX and Linux data types. Refer to **Help** for more information about Reports.

Configuring vCenter Server Data Collections

Collecting vCenter Server data is based on a process that is different from the standard collection process. This process has several prerequisites that must be in place. When the prerequisites are met, data is collected from vCenter Server using Windows Remote Commands.

The collected vCenter Server data is displayed in **Console** | **Virtual Environments** | **vCenter** and **Console** | **Virtual Environments** | **VM Hosts** | **User and Groups**.

vCenter Server Collection Prerequisites

To configure the Collector for vCenter Server collections you must perform the following prerequisites.

IMPORTANT The following steps must be performed in the order presented.

Removing PowerShell v1.x on the VCM Collector

This step can be performed before or after installing VCM.

1. Go to **Add/Remove Programs**.
2. Select **Show Updates**. The list displays updates associated with installed programs.
3. Look for any of the following KB numbers, which indicate earlier versions of PowerShell. Versions of v1.x prior to RC2 are MS-based installations. These versions will appear as Windows PowerShell in the programs list.
   - KB926139 - Windows PowerShell v1.0 RTM - English Language Version
   - KB926140 - Windows PowerShell v1.0 RTM - Localized Installation Package
   - KB926141 - Windows PowerShell v1.0 RTM - MUI pack
   - KB925228 - Windows PowerShell v1.0 RC2
4. Uninstall any occurrence of PowerShell v1.x.

Downloading and Installing PowerShell v2.0 on the Collector

This step can be performed before or after installing VCM.

Click the following link, and then download and install the appropriate version of PowerShell 2.0, included in the Windows Management Framework: http://support.microsoft.com/kb/968929.

Instructions for properly configuring PowerShell are provided later in this procedure.

Downloading and Installing VMware vSphere PowerCLI on the Collector

Click the following link, and then download and install the VMware vSphere PowerCLI 4.0 or 4.1. You will be required to register on the VMware Web site.

http://www.vmware.com/support/developer/PowerCLI/index.html

Configuring PowerShell on the Collector

On the Collector machine, configure the PowerShell execution policy. This step can be performed before or after installing VCM. If you are running a 64-bit collector, you must run the command in PowerShell (x86).

1. Select **Start | All Programs | Accessories | Window PowerShell | Windows PowerShell**. The **Windows PowerShell** window appears.
2. At the prompt, type one of the following. The command you use depends on your local policies.
   - Set-ExecutionPolicy RemoteSigned
   - Set-ExecutionPolicy AllSigned
3. Press **Enter**. The command is executed.

Configuring User Credentials

These steps can be performed only after installing VCM.

The user account used to run the vCenter Windows Remote Commands must load credentials from files created by this user, and cannot be accessed by any other user. If this user is not authorized when creating the import helper object, the data is not inserted into the VCM database.

Creating or Selecting a Network User for vCenter Server Collections

Create of select a network user to use with local administrator privileges on the Collector.

Configuring VCM User Credentials

Create a user in VCM with the Admin role assigned.

Configuring the EcmAgtStartup Identity

1. On the Collector, select **Administrative Tools | Component Services**. The **Component Services** window appears.
2. Expand **Component Services | Computers | My Computer | DCOM Config**.
3. Right-click **EcmAgtStartup**, and then select **Properties**. The **EcmAgtStartup Properties** dialog box appears.
4. Click the **Identity** tab.
5. Select **This user**, and then type or select the user with the VCM Admin privileges required for vCenter Server collections.
6. Type the assigned password in the **Password** and **Confirm** password text boxes.
7. Click **OK**, and then close the Component Services window.

Configuring the Remote Commands PowerShell Credentials

In order to collect from a vSphere vCenter 4 instance you must set credentials. You will need to set the credentials that allow VCM to connect to vCenter Server as well as to the individual, licensed ESX hosts managed by the vCenter Server instance.

If passwords change in the future, simply run the script again, replacing the contents of the existing file.

1. If you are logged on locally as the EcmAgtStartup user, you can go directly to opening the command prompt. Select **Start | Run**, and then type `cmd.exe`. Otherwise, perform the following steps:
   a. If you are not logged on locally to the Collector machine as the EcmAgtStartup user, right-click `C:\WINDOWS\system32\cmd.exe` and select **Run As**. The **Run As** dialog box appears.
   b. Clear the **Run this program with restricted access** check box.
   c. Select **The following user** and configure the **User name** and **Password** to use the same user as EcmAgtStartup.
   d. Double-click `cmd.exe` to open the command prompt.
2. In the command prompt, type the following:

   ```
   cd "C:\Program Files\VMware\VCM\WebConsole\L1033\Files\Remote_Command_Files"
   powershell.exe
   .\Save_MachinePSCredential.ps1
   ```

   where `C:\Program Files\VMware` is replaced with your local path if it differs.
3. Press **Enter**.
4. The prompt displays the following:

   You must be running PowerShell as the user configured for the EcmAgentStartup DCOM object. Would you like to continue? [Y] or [N]
5. Type **Y**, and then press **Enter**.
6. Update the following as requested:
   - **Machine name:** Type the name of the vCenter Server machine from which you are collecting.
   - **UserName:** Type the user name used to connect to this machine. This is also the machine name used in the Remote Commands script.

- **Password:** Type the password associated with the user name.

7. After specifying the password, the script runs, creating a `<MachineName>.txt` file in the user's `C:\Documents and Settings\<username>\Application Data\VCM PowerShell Credentials` folder.

NOTE The credentials are securely saved as `<machine name>.ps1` to the user's profile in a "VCM PowerShell Credentials" folder. These files are accessible only to this user. Any other user reading the file will not be able to decrypt the contents. The file is protected by the Windows DPAPI. If moved, copied, or changed it will cease to function.

8. Run the `.\Save_MachinePSCredential.ps1` script again to set credentials for additional machines. You will also need to do this for any licensed ESX hosts managed by this vCenter Server. In this case, you will need to match the machine name used by vCenter Server, not VCM.

TIP If you receive errors, right-click **Run-As** on the cmd.exe and clear the "Run this program with restricted access" check box, even if you are logged in with the EcmAgentStartup user.

License vCenter Server Machines as Windows Machines in VCM

The Windows machine running vCenter Server must be licensed in VCM in order to collect data from the machine and to collect data from vCenter Server.

Cloning and Configuring the vCenter Remote Commands Templates

The vCenter Collection folder contains four template files by default. These files should not be modified; instead you should clone the files to meet your local needs.

The cloned files you create are the mechanism used to collect vCenter Server data from the ESX/vSphere Server machines. The collected data classes in VCM are vCenter Host Profiles, Host Status, and Inventory, displayed at **Console | Virtual Environments | vCenter**, and Users and Groups, displayed at **Console | Virtual Environments | VM Hosts | Users and Groups**. Each of the above data types require a unique remote command file for each machine running vCenter Server; therefore, if you have two machines running vCenter Server, you should create a Machine 1 and Machine 2 version of all four command files, resulting in eight newly cloned and modified files. Remember, do not modify the templates.

The following steps provide only one example, the process applies when you are cloning any of the templates.

1. Select **Console | Windows Remote Commands | vCenter Collection**. The **vCenter Collection** remote commands data grid displays the current remote commands.
2. Select **(TEMPLATE) vCenter Host Profiles collection - {server name here}**, and then click **Clone**. The **Name and Description** wizard page displays *Copy_1_of_(TEMPLATE) vCenter Host Profiles collection - {server name here}* in the **Name** text box and cloning instructions in the description box.
3. In the **Name** text box, revise the name to reflect the name of the vCenter Server from which you are collecting. For example, `vCenter Host Profiles collection - vcenterserver1.local`.
4. Review the information in the **Description** text box, and then revise as needed.
5. Click **Next**. The **Remote Command** page appears.

6. In the **Command Text** text box, revise the script as specified in the description on the previous page. Clone this remote command for each vCenter Server to collect vCenter Host Profiles data from. Replace the "{server name here}" with the vCenter Server to collect from and replace the "SERVER NAME HERE" in the VBScript with the same server name.

   For example, the following default text:

   ```
   Sub DoWork()
       Const server = "SERVER NAME HERE"
       Const dataClassName = "vCenterHostProfiles"
   ```

   becomes:

   ```
   Sub DoWork()
       Const server = "vcenterserver1.local"
       Const dataClassName = "vCenterHostProfiles"
   ```

7. Continue through the wizard without modifying any other settings.
8. Click **Finish**. The new vCenter Collection remote command is added to the list. For example, vCenter Host Profiles collection - vcenterserver1.local is added to the list.
9. Repeat the process for the other templates and other machines.

Collecting vCenter Server Data

Data collection from vCenter Servers requires you to run remote commands rather than use the Collection wizard. This option is used when you want to run an individual collection for the vCenter Server data. To run the remote commands, use one of the methods described in this section.

The vCenter Remote Commands are run only against the VCM Collector, not the vCenter Servers. The scripts collect the data and update the VCM database.

After validating the collection process using one of the methods below, you have the option to create a scheduled job to automatically collect vCenter Server data. See the Help for more information.

Collecting vCenter Server Data Using the Remote Command Toolbar Button

1. On the portal toolbar, click **Remote Command**. The **Run Remote Command** wizard appears.
2. Select **Windows Remote Command**, and then click **Next**. The **Machines** page appears.
3. Select the Collector machine only. DO NOT select the vCenter Server machines. To select the Collector, double-click the machine in the upper pane to add it to the lower pane.
4. Click **Next**. The **Remote Commands Folder** page appears.
5. Expand the Windows Remote Commands folder and select the **vCenter Collection** folder.
6. Click **Next**. The **Remote Commands** page appears.
7. In the **Available** list, locate the cloned command created for the machine and with the desired collection type, and then double-click the file name to add to the **Selected** list. You can add more than one collection command to the Selected list. Running more than one command allows you to collect all the data from a particular vCenter Server. The commands are run in the order listed.
8. Click **Next**. The **Schedule** page appears.
9. Select one of the following schedule options.

- **Run Action now:** Runs the job immediately when you finish the wizard.
- **Schedule the Action to run later:** Runs the job based on the time and date that you enter.
  - **Time:** To specify a time for the job, enter the time in the time field, and then click **AM** or **PM**.
  - **Date:** To specify a date for the job, use the Calendar.

10. Click **Next**. The **Confirmation** page appears.
11. Review the information and click **Finish**. The selected vCenter Collection remote commands run at the scheduled time.

Collecting vCenter Server Data using Windows Remote Commands

1. Select **Console | Windows Remote Commands | vCenter Collection**. The data grid displays the available vCenter commands.
2. Select a command based on the collection type and machine name.
3. Click **Run**. The **Machines** page of the Remote Commands wizard appears.
4. Select the Collector machine only. DO NOT select the vCenter Server machines. To select the Collector, double-click the machine in the **Available** list to add it to the **Selected** list.
5. Click **Next**. The **Schedule** page appears.
6. Select one of the following schedule options.
   - **Run Action now:** Runs the job immediately when you finish the wizard.
   - **Schedule the Action to run later:** Runs the job based on the time and date that you enter.
     - **Time:** To specify a time for the job, enter the time in the time field, and then click **AM** or **PM**.
     - **Date:** To specify a date for the job, use the Calendar.
7. Click **Next**. The **Important** page appears.
8. Review the information and click **Finish**. The selected vCenter Collection remote command runs at the scheduled time.

Reviewing Collected vCenter Server Data

Collected vCenter Server data is displayed in the following locations:

Console | Virtual Environments | vCenter

Host Profiles

Host Status

Inventory

Console | Virtual Environments | VM Hosts | User and Groups

Troubleshooting vCenter Server Data Collections

If no data appears in the vCenter Server data grids, review the following troubleshooting options:

- You have not created the credential file for this machine (for example, vcenterserver1.local).
- You did not create the credential as the correct user (use Run-as on Cmd.exe as EcmAgtStartup Identity)
- You did not specify a valid vCenter Server instance.
- None of the machines for which data was found were licensed.
- In some cases, like Host Users and Groups, you must have credential files for the ESX/vSphere Servers as well.
- The EcmAgtStartup user is not configured as an Admin in VCM.

More advanced troubleshooting options:

- Open the EcmDebugEventViewer and set the Filter to "Use Custom Sql Where Clause" = "[class_name] = 'ScmHelperAppPowerShell'". Look for any errors or exceptions. It may be beneficial to turn on Info logging in order to get full debug out of the helper app's output. The ScmHelperAppPowerShell is the code responsible for parsing the returned Xml from PowerShell and importing it into VCM.

About the vSphere Client VCM Plug-in

The vSphere Client VCM Plug-in is a tool that provides VCM functionality to vSphere Client users. The integration allows vSphere Client users to utilize VCM's powerful data collection capabilities to manage Compliance, Assessment, and Reporting on Virtual Machines commonly managed in the vSphere Client.

The vSphere Client VCM Plug-in provides contextual access to VCM 's change, compliance, and management functions, in addition to direct access to vCenter, and Host and Guest dashboards.

CAUTION Each user accessing VCM and the vSphere Client should have a unique login. Do not share vSphere Client logins between VCM users, and do not share vSphere Client logins between VCM users and non-VCM users.

Registering the vSphere Client VCM Plug-in

The registration process configures the URL to the VCM server in the VMware vSphere Client, and makes the VCM Summary and VCM Actions tabs available in the vSphere Client.

The plug-in is installed automatically with VCM. Follow the steps below to register the Plug-in with the vSphere Client. To un-register a previous version of the Plug-in, see the steps in Upgrading the vSphere Client VCM Plug-in.

IMPORTANT The account being used to register the vSphere Client VCM Plug-in should be a local administrator on the vSphere instance. The account should be connecting to a machine that has a valid SSL certificate, or must register an invalid certificate (for example, a development certificate) when that user logs into the vSphere Client.

Requirements

The requirements for the vSphere Client VCM Plug-in include:

- VMware vCenter 4 Server
- VMware vSphere Client
- VMware Tools installed on Virtual machines

To register the vSphere Client VCM Plug-in:

1. On the VCM Collector, browse to:
   `[path]\VMware\VCM\Tools\vSphere Client VCM Plugin\bin`
2. Double-click `VCVPInstaller.exe`. The **VCVP Plug-in Registration** dialog box appears.
3. Configure the following options:
   - **Register:** Select the option to register the URL for the plug-in. (Select Unregister only if you are discontinuing the use of the plug-in on the target vSphere Client.)
   - **Server URL:** Type the http or https path, where <server> is your vSphere Client server.
   - **Administrator User Name:** Type the name of a user with Administrator privileges in the vSphere Client.
   - **Administrator Password:** Type the associated password.
   - **URL to vSphereClientVCMPlugin.xml:** Type the http path, where <VCMserver> is the name or IP address for the VCM Collector. The xml file is named `vSphereClientVCMPlugin.xml`, and is located in `\VMware\VCM\WebConsole\L1033\VCVPAnon\Xml\`.
4. Click **OK**.
5. Start VCM. On the login screen, select the role you are using to log into the vSphere Client VCM Plug-in. Select the **Automatically log in using this role** check box. This action ensures that the selected role is used to log into the Plug-in located in the vSphere Client.
6. Start the vSphere Client.
7. Select a Guest machine. The displayed tabs should include **VCM Summary** and **VCM Actions**. You are ready to use the vSphere Client VCM Plug-in.
8. After confirming you can access the **VCM Summary** and **VCM Actions** tabs, you must configure the vSphere Client VCM Plug-in integration settings in VCM. Click **Administration** | **Settings** | **Integrated Products** | **VMWare** | **vSphere Client VCM Plug-in**.

Troubleshooting the vSphere Client VCM Plug-in Registration

If the VCM Summary and VCM Actions tabs are not displayed, one of the following problems may have occurred:

- https/SSL is not configured on the VCM Collector, but **Use SSL** was selected during VCM installation. Steps to resolve:
  1. Open the xml file specified during the registration.
  2. Edit the file to reflect the configured connection method, either http or https.
- The Plug-in is not enabled. Steps to resolve:
  1. In the vSphere Client, select **Plug-ins** | **Manage Plug-ins**. The **Plug-in Manager** appears.
  2. In the **Installed Plug-ins** area, right-click the vCenter Configuration Manager Extension plug-in, and select **Enable**.
  3. Close the Plug-in Manager. When the tabs appear, you are ready to use the vSphere Client VCM Plug-in.

Configuring the vSphere Client VCM Plug-in Integration Settings

Perform these steps to configure integration settings for vSphere Client VCM Plug-in users. The settings configured in this area enable users to view the VCM reports.

1. Select **Administration | Settings | Integrated Products | VMware | vSphere Client VCM Plug-in**.
2. Select the setting you want to configure, and then click **Edit Settings**.
3. The **Settings Wizard** page appears. The information to be configured will vary depending on selected setting. Configure the options as follows:
   - **Machine group against which the external reports will be run:** Type the name of the machine group. The default value is All Machines.
   - **Role to use for external report access:** Type the name of the user role to be used to access the reports. The default value is Read-Only. Users other than Admin must have the role selected here in order to see reports in the vSphere Client.
   - **User name to use for assessments:** Identifies the user who will be running assessments to obtain data for generating reports.
4. Click **Next**.
5. Verify your settings, and then click **Finish** to apply the settings.

Getting Started with the vSphere Client VCM Plug-in

The vSphere Client VCM Plug-in provides integration with VCM to VMware vSphere Client users. The integration allows vSphere Client users to utilize VCM's powerful data collection capabilities to manage Compliance, Assessment, and Reporting on Virtual Machines commonly managed in the vSphere Client.

Working with an Invalid Certificate on a vSphere Client

When logging into a vSphere Client for the first time, if the certificate is not valid, a security warning about the SSL certificate appears. To install the SSL certificate, follow these steps.

1. Check the option: "**Install this certificate and do not display any security warnings for <vCenter_Server_Instance>**".
2. Click **Ignore**.

The vSphere Client connects to the vCenter Server using the SSL certificate, and displays the datacenters, hosts, and any clusters.

Getting Started with the vSphere Client VCM Plug-in

Use the following workflow to begin working with the vSphere Client VCM Plug-in when adding vSphere Client-managed machines to the VCM database. See the online **Help** for details.

1. License Windows and UNIX\Linux machines.
   - Licensing Windows Guest machines
   - Licensing UNIX Guest machines
2. Install the Agent, either Windows or UNIX\Linux.
   - Installing the Agent on Windows Guest machines
   - Installing the Agent on UNIX Guest machines
3. Start the vSphere Client and begin collecting data. Click **Help** and the **VCM Actions** tab for more information.

Upgrading the vSphere Client VCM Plug-in

The vSphere Client VCM Plug-in integrates VMware vCenter Configuration Manager into the vSphere Client to provide VCM data and functionality within vCenter. After upgrading VCM, you must upgrade the Plug-in, which means vCenter users must un-register it and then re-register it.

Upgrading the Plug-In

To upgrade the vSphere Client VCM Plug-in, follow these steps:

1. Upgrade VCM.
2. Manually un-register the pre-VCM 5.3 version of the Plug-in, as described in Un-register the Previous Version of the Plug-in in Un-register the Previous Version of the Plug-in.
3. Register the new Plug-in by following the instructions in "Registering the vSphere Client VCM Plug-in" on page 143.

Un-register the Previous Version of the Plug-in

If you have already upgraded VMware vCenter Configuration Manager, you must manually un-register the previous version of the Plug-in before registering the VCM 5.3 Plug-in. Although the upgrade to VCM removes files for the previous Plug-in, and installs the new Plug-in files in new locations and with new names, it does not register the new Plug-in with the vSphere Client. To un-register the existing Plug-in, follow these steps.

1. Browse to the following link, where "`{vCenter machine name}`" is the name of your vCenter 4 Server instance:
   `https://{vCenter machine name}/mob/?moid=ExtensionManager`
2. In the **Methods** area, click the **UnregisterExtension** link.
3. Enter the following string value for **extensionKey**: **com.CM.VirtualCenterCompliancePlugIn**
4. Click **Invoke Method**.

Further Reading

Refer to Customizing VCM for information on how to customize for your environment. Several of these areas regarding customization also apply to VCM. You can also read Maintaining VCM after Installation for important information regarding additional data retention settings and database maintenance steps which should be taken.

When using VCM, refer to online **Help** for specific information. For information about upgrading, see Upgrading VCM for Virtualization.

Getting Started with VCM Remote 7

Getting Started with VCM Remote

Many workstations come and go from the network. This transient behavior is especially true of mobile workstations, such as laptops. From a mobile workstation, you can connect by dialing in, connect from a client site via a Virtual Private Network (VPN), or connect from an alternate location via a DSL line or cable modem. In these scenarios, these devices may connect over networks with variable available bandwidth such as:

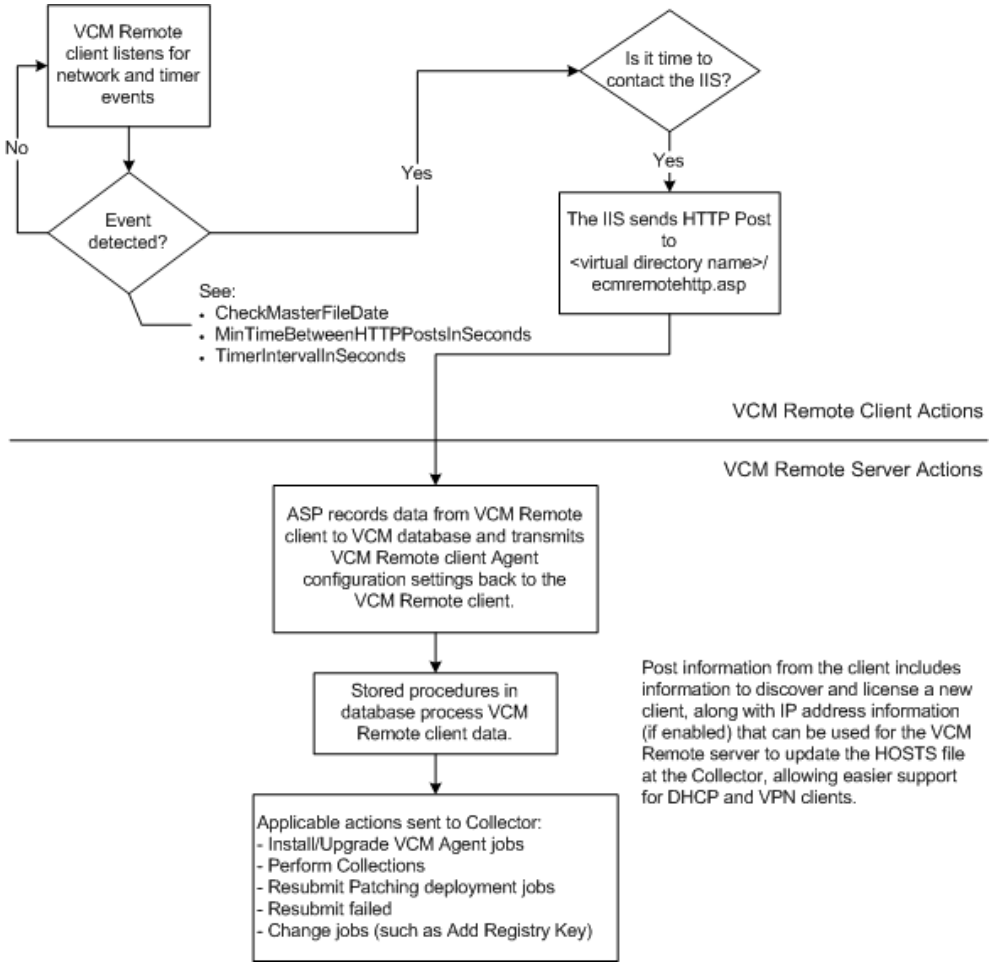
- **Broadband:** DSL and cable connections can be 156 Kb to more than 1 Mb
- **Dialup:** A dial-up connection could be 56 Kb or less
- **LAN:** A local area connection to the network equal to or greater than 1 Mb. A VPN connection may be at LAN speeds but connected over the Internet

Machines may not be, and often are not, on the network when the Collector initiates a collection. Consider patch management. You need up-to-date information to perform the Assessments to ensure your machines and production networks are protected from the latest vulnerability. Relying on data from mobile workstations can be risky.

The VCM Remote client provides support for mobile Windows workstations. VCM Remote is a service-based agent that "announces" itself when it is online. The agent sends this announcement over HTTP to a server-side component residing on the VCM Internet Information Services (IIS) server. Based on user-defined settings on the IIS server, the Collector creates immediate requests, such as collections, for the machine that just came online. The server-side processing is smart enough to batch work at periodic intervals. This technique avoids the problem of having 15,000 clients come online within ten minutes of one another and creating 15,000 individual requests.

Workflow Diagram

The basic sequence of actions is represented in the following diagram.


VCM Remote client listens for network and timer events
Is it time to contact the IIS?
No
Yes
Yes
Event detected?
The IIS sends HTTP Post to <virtual directory name>/ ecmremotehttp.asp
See:
• CheckMasterFileDate
• MinTimeBetweenHTTPPostsInSeconds
• TimerIntervalInSeconds
VCM Remote Client Actions
VCM Remote Server Actions
ASP records data from VCM Remote client to VCM database and transmits VCM Remote client Agent configuration settings back to the VCM Remote client.
Stored procedures in database process VCM Remote client data.
Post information from the client includes information to discover and license a new client, along with IP address information (if enabled) that can be used for the VCM Remote server to update the HOSTS file at the Collector, allowing easier support for DHCP and VPN clients.
Applicable actions sent to Collector:
- Install/Upgrade VCM Agent jobs
- Perform Collections
- Resubmit Patching deployment jobs
- Resubmit failed
- Change jobs (such as Add Registry Key)

Before Collecting Remote Data

Begin using VCM Remote by following the steps outlined below. For more information, click any step to jump to the related section.

Step 1: Installing VCM Remote Client

Step 2: Making VCM Aware of VCM Remote Clients

Step 3: Configuring the VCM Remote Settings

Step 3a: Creating Custom Collection Filter Sets

Step 3b: Specifying Custom Filter Sets in the VCM Remote Settings

Step 4: Performing a Collection Using VCM Remote

Step 5: Reviewing the VCM Remote Collection Results

Installing the VCM Remote Client

Installing VCM Remote involves installation of both the VCM Remote server and VCM Remote Client. The VCM Remote server was installed when the VCM Installation Manager was run. The VCM Remote Client must be installed separately.

The VCM Remote Client can be installed using any of several methods, including a manual installation (provided below), "Installing the Remote Client using a Command Line" on page 151, or "Installing the Remote Client using Windows Remote Commands" on page 152. All the methods are described in this section.

Additionally, communication between the Collector and the Remote Client is secured using Transport Layer Security (TLS) certificates. You can use the Enterprise certificate generated by VCM or you can use an existing Enterprise certificate. The steps below include copying the VCM generated certificate to the Remote Client; however, if you have an existing Enterprise certificate in the certificate store with a known trust relationship with the Collector, you do not need to perform those steps. By default, the installation of a Windows VCM base agent in HTTP mode adds the Collector's Enterprise Certificate to the certificate store of the client system, and this certificate can also be used by the VCM Remote client.

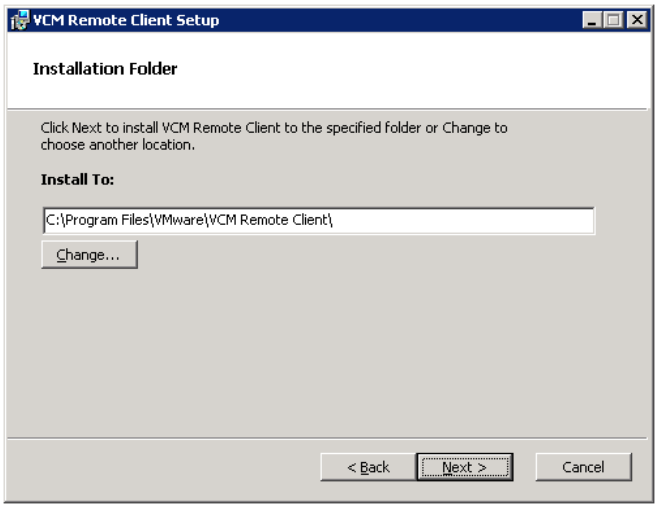
NOTE The VCM Remote Client can be deployed to multiple machines in your enterprise using VCM's Remote Command feature. See "Installing the Remote Client using Windows Remote Commands" on page 152 for more information.

Installing the Remote Client manually

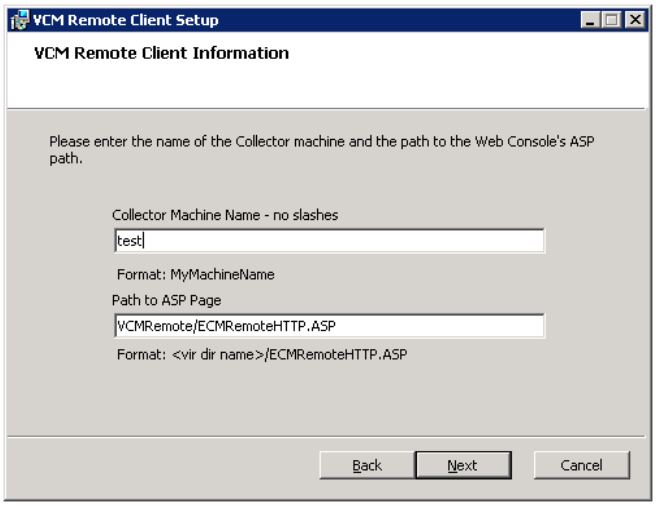
1. Create a folder on the target mobile workstation and copy the following files from the Collector to the target folder:
   - **CM Remote Client.msi**: Located on the Collector at `[install path]\VMware\VCM\AgentFiles`.
   - **CM_Enterprise_Certificate_xxx.pem:** Located on the Collector at `[install path]\VMware\VCM\CollectorData`.
2. Double click the **CM Remote Client.msi** copied to the mobile workstation. The **VCM Remote Client Setup** installation wizard appears.

VCM Remote Client Setup
vmware
Welcome to VCM Remote Client Setup
VMware vCenter
Configuration Manager™
Setup will install VCM Remote Client on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Copyright (C) 1998-2010 VMware, Inc. All Rights Reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
Back
Next
Cancel

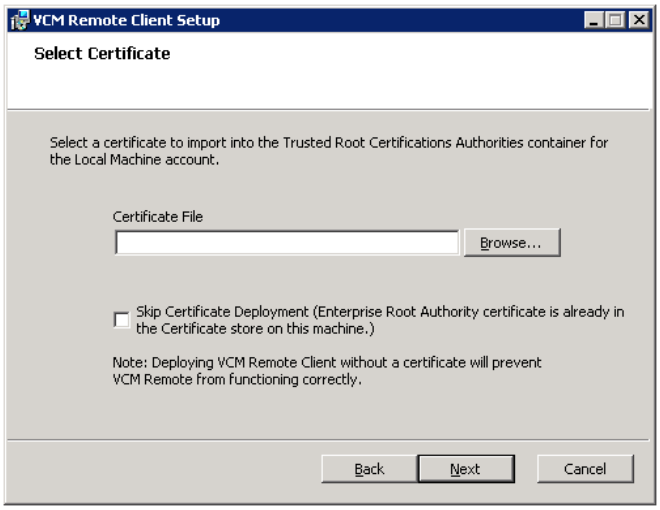
3. Click **Next**. The **Installation Folder** page appears.


VCM Remote Client Setup
Installation Folder
Click Next to install VCM Remote Client to the specified folder or Change to choose another location.
Install To:
C:\Program Files\VMware\VCM Remote Client\
Change...
< Back
Next >
Cancel

4. Accept the default installation location, or click **Change** to enter a different location. Click **Next**.



5. Type the name of the Collector machine and the path to the Web Console's ASP path as follows:
   - **Collector Machine Name:** Type the name of the machine on which the VCM Collector and Microsoft IIS are installed.
   - **Path to ASP Page:** This path was created in the IIS default web site by the VCM Remote server installation. The <virtual directory name> must match the virtual directory name entered when you installed the server component.
6. Click **Next**. The **Select Certificate** page appears.


VCM Remote Client Setup
Select Certificate
Select a certificate to import into the Trusted Root Certifications Authorities container for the Local Machine account.
Certificate File
Browse...
Skip Certificate Deployment (Enterprise Root Authority certificate is already in the Certificate store on this machine.)
Note: Deploying VCM Remote Client without a certificate will prevent VCM Remote from functioning correctly.
Back
Next
Cancel

7. Configure or select one of the following certificate options:
   - If you copied the VCM-generated Enterprise certificate to the CM Remote Client, to locate the certificate (.pem), click **Browse**.
   - If you are using an existing Enterprise certificate in the client certificate store, select **Skip Certificate Deployment**.

   IMPORTANT Do not select **Skip Certificate File Import** unless you are certain the Enterprise certificate exists in the client certificate store. If you select this option, the Remote Client will use the Enterprise certificate in the store. If the certificate does not exist in the store, any communication between the client and the Collector will fail.

8. Click **Next**. The **Ready to install CM Remote Client** page appears.
9. Click **Install** to begin the installation.
10. When the installation is completed, click **Finish**.

NOTE After the Remote Client is installed, the first time the Remote Client connects with the Collector, it requests a Collector certificate. If the Collector certificate is trusted by the Enterprise certificate on the client, the Collector certificate is added to the client's certificate store.

Installing the Remote Client using a Command Line

The VCM Remote Client can be installed using any of several methods, including "Installing the VCM Remote Client" on page 148, Installing the Remote Client using a Command Line (provided below), or "Installing the Remote Client using Windows Remote Commands" on page 152.

1. On the Collector, navigate to the path where you installed the software, which by default is `C:\Program Files\VMware\VCM\AgentFiles`.
2. Copy `CM Remote Client.msi` to the target mobile workstation.
3. On the Collector, navigate to the path where you installed the software, which by default is `C:\Program Files\VMware\VCM\CollectorData`.
4. Copy the certificate file (.pem) to the target mobile workstation.
5. On the workstation, open a command prompt and type the following command:

```
msiexec.exe /qn /i "[path]\cm remote client.msi" COLLECTOR="YourCollectorName"
 PATHTOASP="VCMRemote/ecmremotehttp.asp" INSTALLDIR="c:\Program
Files\VMware\VCM Remote Client” CERTIFICATE_
FILE="[path]\YourEnterpriseCertificateName.pem" /log "[path\]filename.log"
```

NOTE If the names and paths contain spaces, you must use double quotation marks. See the example above.

Where:

/qn: No error messages are displayed.

[path]\cm remote client.msi: Specify the path to the CM Remote Client.msi on the target machine.

COLLECTOR=YourCollectorName: Replace <YourCollectorName> with the name of your VCM Collector.

PATHTOASP=VCMRemote/ecmremotehttp.asp: If necessary, replace VCMRemote (the default virtual directory name) with the name of the IIS Default Web Site virtual directory containing ecmremotehttp.asp.

INSTALLDIR:c:\Program Files\VCM\CM Remote Client: Specify the path where you want the Remote client files installed on the target machine. The directory will be created by the command.

CERTIFICATE_FILE=[path]\YourEnterpriseCertificateName.pem: Specify the path and the certificate name on the target machine.

NOTE If you are using an existing Enterprise certificate in the client certificate store, you can use SKIP_CERTIFICATE_FILE=1 instead of CERTIFICATE_ FILE=YourEnterpriseCertificateName.pem.

IMPORTANT Do not use this option unless you are certain the Enterprise certificate exists in the client certificate store. If you specify SKIP_CERTIFICATE_FILE=1, the Remote Client will use the Enterprise certificate in the store. If the certificate does not exist in the store, any communication between the client and the Collector will fail.

/log [path\]filename.log: Any error messages are added to the log file. If a path is specified, the log file is saved to that location. If the path is not specified, the log file is saved in the directory from which the msiexec.exe was run. The log files are a useful troubleshooting tool.

Installing the Remote Client using Windows Remote Commands

The VCM Remote Client can be installed using any of several methods, including a "Installing the VCM Remote Client" on page 148 (a manual installation), "Installing the Remote Client using a Command Line" on page 151, or Installing the Remote Client using the Window Remote Commands (provided below).

Before you can run the Remote Command, you must have the VCM Agent installed on the target Remote machine.

NOTE Using this option, the VCM Remote Client can be deployed to multiple machines in your enterprise.

1. On your VCM Collector, copy ...\VMware\VCM\AgentFiles\CM Remote Client.msi to...\VMware\VCM\WebConsole\L1033\Files\Remote_Command_Files.
2. On your VCM Collector, copy ...\VMware\VCM\CollectorData\<YourEnterpriseCertificate>.pem to the same location specified in step 1 (to...\VMware\VCM\WebConsole\L1033\Files\Remote_Command_Files).
3. In VCM, select **Console | Windows Remote Commands**.
4. Click **Add**. The **Remote Commands** wizard appears.
5. Type the **Name** and **Description** of the your new command.
6. Click **Next**. The **Remote Command** page appears.
7. In the **Type** drop-down list, select VBScript.
8. In **Command Text** text box, copy and paste the following Script. Modify the script as specified in the comments of the script.

NOTE The script installs the Remote Client under the Windows directory rather than the Program Files directory. It is not necessary to create the install directory on the target machine before running the script.

```
Call DoWork

'Copyright 1999-2010 VMware, Inc.

'Coded by Ryan L.

'Description: Installs VCM Remote ver. 2

'Modified 4/27/2008 - Stephen S. Included Certificate file options

'Modified 7/7/2010 - VCM

Dim sCollName, sInstallDir, sVirDir, sAddRemove, sCertFile, bInstallCert

Sub DoWork()

Set WshShell = CreateObject("WScript.Shell")

sCollName = "YourCollectorName" 'Name of your VCM Collector machine in
quotes

bInstallCert = 1 'If the value is 1, the Enterprise Certificate is
installed. If the value is set to 0, the installation of the certificate
is skipped and it is assumed that the certificate is already present. The
Remote Client will NOT function until the Enterprise Certificate is
installed as specified in Step 2

sCertFile = "EnterpriseCert" 'The filename of your enterprise certificate
 (.pem file) as identified in Step 2

sVirDir = "VCMRemote/EcmRemoteHttp.asp" 'Where you replace CMRemote with
the IIS Default Web Site virtual directory containing the
ECMRemoteHTTP.asp file

sInstallDir = WshShell.ExpandEnvironmentStrings("%windir%") &
"\VMware\VCM Remote Client" 'The installation directory on the TARGET
machine
```

```
sAddRemove = 1 'Whether or not VCM remote should appear in the Add/Remove
programs List, should be 0 = hide, 1 = show

sMSIPackageName = "CM Remote Client.msi" 'Name of the MSI package that
installs VCM Remote Agent


CheckVars


If sAddRemove = 0 Then

AppToRun = "msiexec.exe /qn /i " & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & "
ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" &
Chr(34) & sVirDir & Chr(34) & " ARPSYSTEMCOMPONENT=" & sAddRemove & "
INSTALLDIR=" & Chr(34) & sInstallDir & Chr(34)

Else

AppToRun = "msiexec.exe /qn /i " & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & "
ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" &
Chr(34) & sVirDir & Chr(34) & " INSTALLDIR=" & Chr(34) & sInstallDir &
Chr(34)

End If

If bInstallCert = 1 Then

AppToRun = AppToRun & " CERTIFICATE_FILE=" & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sCertFile & Chr(34)

Else

AppToRun = AppToRun & "SKIP_CERTIFICATE_FILE=1"

End If

EcmScriptRuntime.CmdExecute Chr(34) & AppToRun & Chr(34), 10000

End Sub


Sub CheckVars()

If sCollName = "" Then

WScript.Quit

Else

sCollName = Trim(sCollName)

End If


If sVirDir = "" Then

sVirDir = "vcmremote/ecmremotehttp.asp"

Else
```

```
sVirDir = Trim(sVirDir)
End If

If sInstallDir = "" Then
sInstallDir = "c:\vcm remote client"
Else
sInstallDir = Trim(sInstallDir)
End If

If sAddRemove <> 0 And sAddRemove <> 1 Then
sAddRemove = 1 'Set whether or not VCM Remote appears in the Add/Remove
programs list. 1=display, 0=do not display
End If

If sAddRemove = "" Then
sAddRemove = 1
End If

If IsNumeric(sAddRemove) = False Then
sAddRemove = 1
End If

sAddRemove = Trim(sAddRemove)
End Sub
```

9. Select the **Certain file(s) are required to be on the target machine for this remote command** check box.
10. Click **Next**. The **Files** page appears.
11. Select the `CM Remote Client.msi` file and the `.pem` file then move them to the right box
12. Click **Next**. When you are ready to save the new remote command, click **Finish**. The command is saved and added to the **Windows Remote Commands** list.
13. To run the new remote command to install VCM Remote Client, select your new remote installation remote command and click **Run**. The **Windows** page of the **Remote Commands** wizard appears.
14. Select the machines on which you are installing VCM Remote.

NOTE The VCM Agent must already be installed on the target machines.

---

15. Click **Next**. The **Schedule** page appears. Select one of the following options:

- **Run Action now:** This option immediately installs VCM Remote Client on the target machines.
- **Schedule the Action to run later:** This option allows you to specify the **Time** and **Date** for the installation.

NOTE The job appears in the Instant Collection job history queue as **Install CM Remote Client**.

16. Click **Next**. When you are ready to proceed, click **Finish**.

Making VCM Aware of VCM Remote Clients

After the VCM Remote Client is installed, the client contacts the collector when connected to the network.

The default VCM Remote setup enables VCM Remote to automatically contact the Collector, auto-license the machine, install or upgrade the base VCM Windows Agent, and determine whether it should submit a VCM collection job for that machine. In addition, VCM Remote resubmits failed deployment jobs if you are using other VCM components for your patch management processing.

This process is automated based on VCM Remote Settings and other than configuring the settings, requires no operator interaction.

Configuring VCM Remote Settings

Once the VCM Remote client and server components have been installed successfully, you need to collect from, or push patches to, the mobile Windows workstations. You must configure the following:

- Create custom Collection filter sets to be used when a mobile workstation connects using Dial-up, Broadband, or LAN. We recommend a different Filter Set for each connection type. See "Creating Custom Collection Filter Sets" on page 156 for more information.
- In the VCM Remote settings, enter the names of the filter sets to be used for each type of connection. See "Specifying Custom Filter Sets in the VCM Remote Settings" on page 156 for more information.

Creating Custom Collection Filter Sets

If you have not created any Collection filter sets, you can specify the default set. However, this is an all-encompassing collection that would likely not be able to complete over a dial-up connection. Therefore, you should create filter sets customized to the type of connection that might be used by the mobile workstations: Dial-up, Broadband, or LAN. For example, the dial-up set might be limited to only a few high-importance items and would not include the File System Uploads or Emergency Repair Disk data classes.

1. In VCM, select **Administration | Collection Filters | Filter Sets**.
2. Select **Add Filter Set**.
3. Construct a filter set appropriate for the connection type. Use the Help available in the Filter Set Wizard to configure the filter set.

Specifying Custom Filter Sets in the VCM Remote Settings

For a Collection of the client machine to take place, a Collection Filter Set must be created and its name entered into VCM. You can, of course, enter Default for the automatically-created default set. The same or different Filter Set names can be assigned to each of the three connection types: Broadband, Dialup, and LAN. For instance, if the connection speed is only that of Dialup, you might want to create a smaller Filter Set. If a connection type does not have a Filter Set name assigned, no Collection will be initiated when the connection is at that speed.

1. In VCM, click **Administration** | **Settings** | **General Settings** | **VCM Remote**. The default selection for the Broadband, Dialup, and LAN collection filter settings that VCM Remote will use for connections require you to edit the setting and specify a collection filter.
2. To specify the name of the filter set for each connection, select the setting that you want to change, then click **Edit Setting**. The **General Settings Edit Setting** wizard appears.
3. In the drop-down list, select the name of the filter set to use for the connection. Click **Next**.
4. Confirm that you want to change the name as specified, then click **Finish**.

Performing a Collection Using VCM Remote

After VCM Remote is installed, it will contact the Collector, auto-license the machine, install or upgrade the VCM Windows Agent, and determine whether it should submit a VCM Collection job for that machine.

Exploring VCM Remote Collection Results

Collection results gathered by VCM Remote are displayed in the same way as other data collected from your VCM-managed Windows machines. Refer to"Exploring Windows Collection Results" on page 68 for more information.

In addition to the general Windows data collected using the VCM Remote Client, you should be aware of the data displayed in the **Administration** | **Job Manager** | **History** | **VCM Remote** node. Refer to the information displayed in the node to verify communication between VCM and the VCM Remote Clients running on your Windows machines. Refer to the online Help for more details on the unique capabilities and features of the VCM Remote Client.

Getting Started with VCM Patching 8

Getting Started with VCM Patching

You can use VCM Patching to assess the state of managed Windows and UNIX/Linux machines, and deploy patches on those machines.

The process to assess managed UNIX/Linux machines differs from the process to assess and patch Windows machines. To view the assessment and deployment process for each type of machine, see:

- Getting Started with VCM Patching for Windows Machines
- Getting Started with VCM Patching for UNIX/Linux Machines

For information about other VCM Patching functionality, such as Windows Patch Staging or creating filters for UNIX Patch Assessment results, see the online Help.

Getting Started with VCM Patching for Windows Machines

Welcome to VCM Patching for Windows. Now that you have installed VCM successfully, proceed through the getting started steps to understand how to assess and update your Windows machines.

To get started, follow these steps:

Step 1: Check for updates to bulletins.

Step 2: Perform a collection using the appropriate filters.

Step 3: Launch an assessment.

Step 4: Explore the results.

Step 5: Deploy the patches.

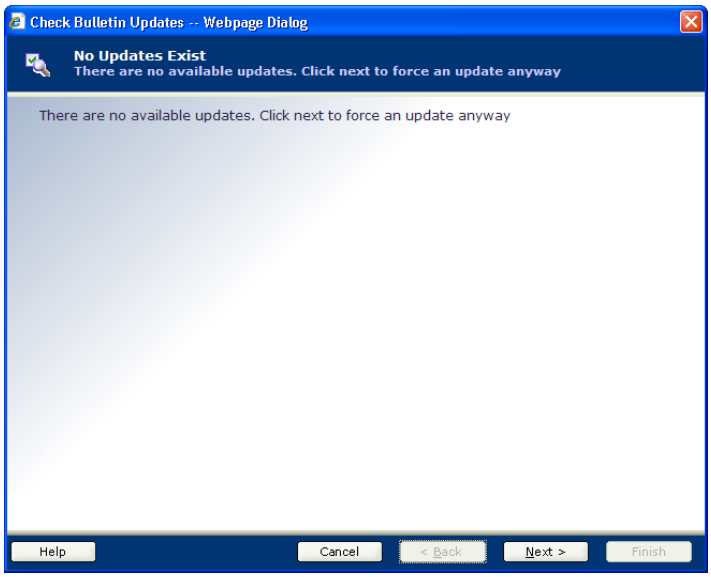
Step 6: Perform another collection.

Step 7: Run another assessment.

Check for Updates to Bulletins

VMware recommends that you use VCM to check for updates to VCM Patching Bulletins prior to creating an assessment template. To check for updates to VCM Patching Bulletins, follow these steps.

1. Click **Patching | Windows | Bulletins**. To obtain a comprehensive view of all released bulletins, click **By Bulletin**. If you know the affected product for which you want to find a bulletin, click **By Affected Product**.
2. Check for updates as follows:
   - **By Bulletin:** Click **Check for Update** in the data grid toolbar.
   - **By Affected Product:** Click the product you want to view, and then click **Check for Update** in the data grid toolbar.


Check Bulletin Updates -- Webpage Dialog
No Updates Exist
There are no available updates. Click next to force an update anyway
There are no available updates. Click next to force an update anyway
Help
Cancel
< Back
Next >
Finish

3. If updates exist, click **Next** to download the updates. VCM displays a dialog box communicating the status of your request. Follow the prompts to either update your bulletins, force an update to the bulletins, or cancel the request.
4. Click **Finish**. The download job is submitted to the pending job queue. When the job completes, the content will be available in VCM.

Collect Data from Windows Machines Using the VCM Patching Filter Sets

The next step is to perform a collection. VCM Patching requires current information about the following Windows data types: File System, Hotfixes, Registry, and Services.

1. On the toolbar, click **Collect**.
2. Select the Windows machines from which to collect data.
3. Mark **Select a Collection Filter Set to apply to these machines**, and then click **Next**.
4. Select the **Patching - Windows Security Bulletins** filter set, and then click **Next**.

NOTE The Patching - Windows Security Bulletins filter set for Windows machines gathers information for all bulletins. However, bulletin filter sets are also available by month. Click any of the monthly filter sets to filter the bulletins released during that month.

---

5. If no conflicts appear, click **Finish** to begin your collection.

NOTE If you experience problems collecting data from your Windows machines via the VCM Patching Filter Sets using the default Network Authority Account, either provide that account with access to the Windows servers or provide a separate Network Authority Account for use with these particular machines. See Default Network Authority Account for more information.

Launch an Assessment

To assess Windows machines, you will **use a template**. The template contains one or more bulletins, and checks the data collected from the machines to confirm whether the patches referenced by the bulletins need to be installed. For example, you might create a template containing all of the bulletins related to Internet Explorer 7 to ensure all of the installed copies have the latest security fixes.

To launch a VCM Patching Assessment, you must:

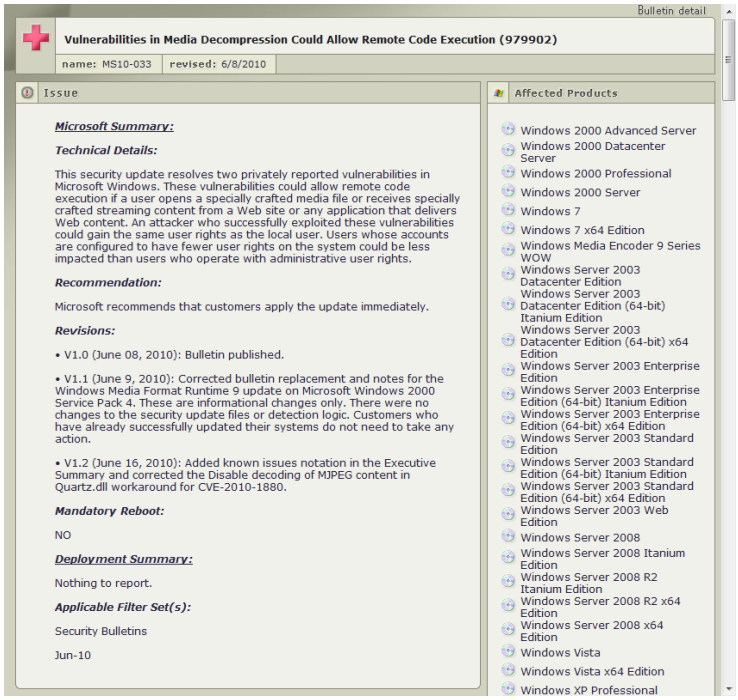
- Review Bulletins to include in the Assessment Template
- Create the Assessment Template
- Run the Assessment

Review Bulletins to include in the Assessment Template

VMware recommends that you review the details of any bulletin before you include it in a VCM Patching assessment.

1. To review bulletin details, select the bulletin that you are interested in, and then click **Details**. VCM Patching displays a bulletin detail dialog box describing the technical details, affected products, and vendor recommendations.

2. Refer to VMware **Deployment Summary** for a list of issues that might impede distribution of a given bulletin.
3. Click **On the Web** to link directly to the vendor's information pertaining to this bulletin.


Bulletin detail
Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)
name: MS10-033
revised: 6/8/2010
Issue
Microsoft Summary:
Technical Details:
This security update resolves two privately reported vulnerabilities in Microsoft Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted media file or receives specially crafted streaming content from a Web site or any application that delivers Web content. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
Recommendation:
Microsoft recommends that customers apply the update immediately.
Revisions:
• V1.0 (June 08, 2010): Bulletin published.
• V1.1 (June 9, 2010): Corrected bulletin replacement and notes for the Windows Media Format Runtime 9 update on Microsoft Windows 2000 Service Pack 4. These are informational changes only. There were no changes to the security update files or detection logic. Customers who have already successfully updated their systems do not need to take any action.
• V1.2 (June 16, 2010): Added known issues notation in the Executive Summary and corrected the Disable decoding of MJPEG content in Quartz.dll workaround for CVE-2010-1880.
Mandatory Reboot:
NO
Deployment Summary:
Nothing to report.
Applicable Filter Set(s):
Security Bulletins
Jun-10
Affected Products
Windows 2000 Advanced Server
Windows 2000 Datacenter Server
Windows 2000 Professional
Windows 2000 Server
Windows 7
Windows 7 x64 Edition
Windows Media Encoder 9 Series WOW
Windows Server 2003 Datacenter Edition
Windows Server 2003 Datacenter Edition (64-bit) Itanium Edition
Windows Server 2003 Datacenter Edition (64-bit) x64 Edition
Windows Server 2003 Enterprise Edition
Windows Server 2003 Enterprise Edition (64-bit) Itanium Edition
Windows Server 2003 Enterprise Edition (64-bit) x64 Edition
Windows Server 2003 Standard Edition
Windows Server 2003 Standard Edition (64-bit) Itanium Edition
Windows Server 2003 Standard Edition (64-bit) x64 Edition
Windows Server 2003 Web Edition
Windows Server 2008
Windows Server 2008 Itanium Edition
Windows Server 2008 R2 Itanium Edition
Windows Server 2008 R2 x64 Edition
Windows Server 2008 x64 Edition
Windows Vista
Windows Vista x64 Edition
Windows XP Professional

NOTE Be sure to view all of the information in the Bulletin Detail window.

Create an Assessment Template

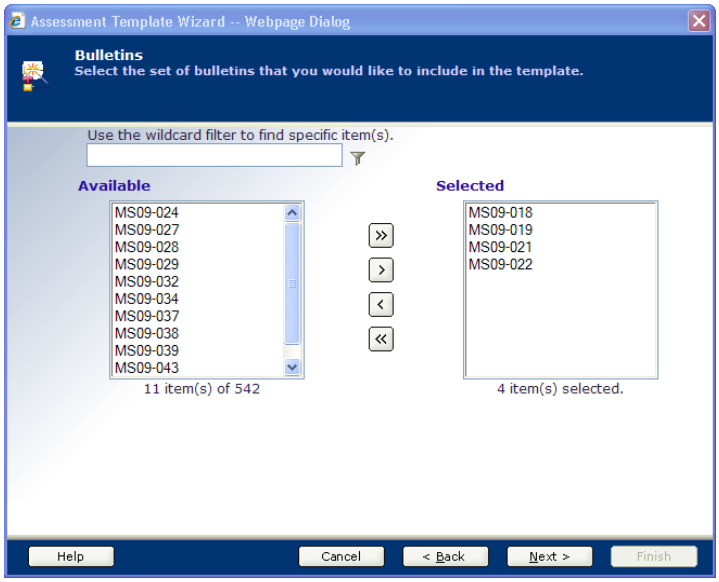
Now that you have checked for bulletin updates and reviewed the details of the bulletins that you want to assess, you can create a template based on those bulletins. Use one of the following methods to create VCM Patching Assessment templates:

- Create a Template Based on a VCM Patching Bulletin
- Create a Template based on a Name

Create a Template Based on a VCM Patching Bulletin

To create a template based on a specific bulletin or group of bulletins, follow these steps.

1. Click **Patching | Windows | Bulletins | By Bulletin**.
2. Select the bulletin to use for the template, and then click **Create Template**. VCM Patching launches the VCM Patching Assessment Template wizard.
3. Type the template name and description in the appropriate fields, and then click **Next**.
4. The bulletin that you selected already appears in the Selected pane. Click **Next**.

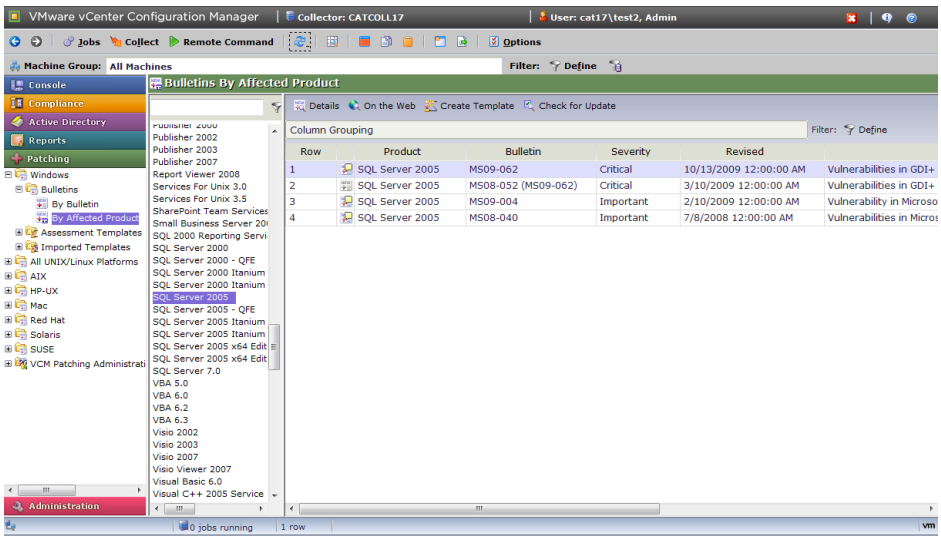


5. Read the confirmation screen, and then click Finish. VCM Patching creates your template and places it in the Assessment Templates folder (**Patching | Windows | Assessment Templates**).

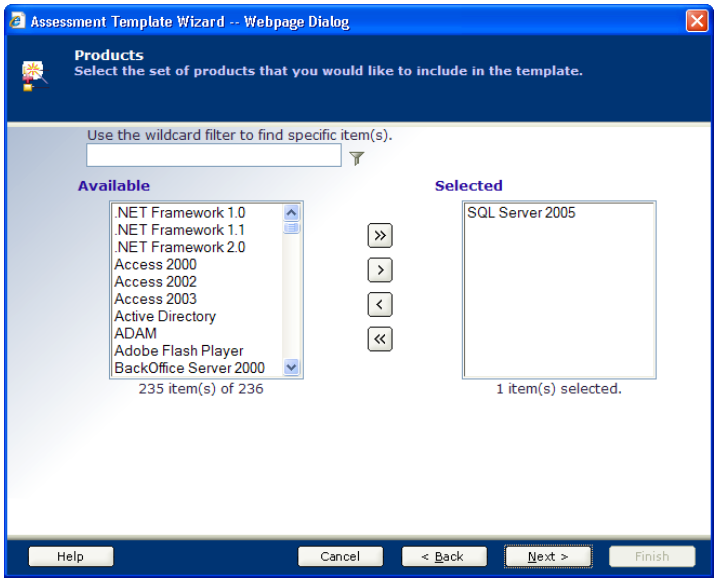
Create an Affected Product Template

To create a template based on bulletins related to a specific product, follow these steps.

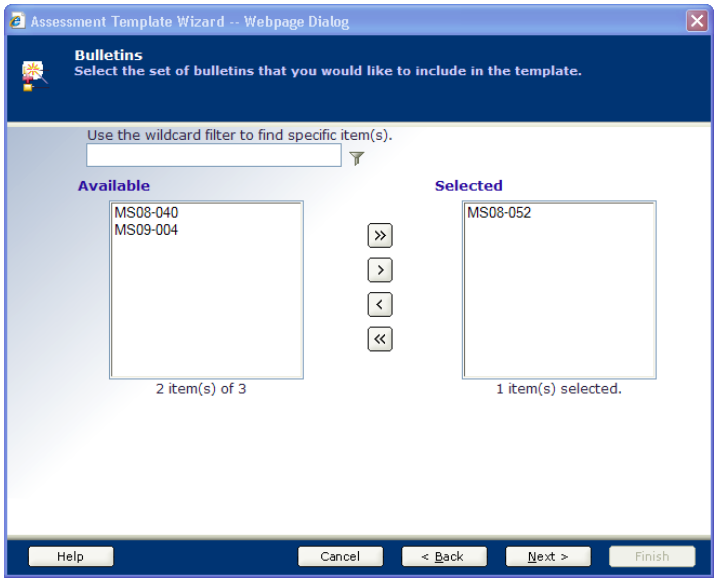
1. Click **Patching | Windows | Bulletins | By Affected Product**.
2. In the middle pane, locate and select the product.



3. In the data grid, VCM displays the bulletins listed by product. Select the bulletin to use for the template, and then click **Create Template**.
4. Type the template name and description, and then click **Next**.
5. The product that you selected appears in the Selected pane. Click **Next**.



6. The bulletin that relates to the product you selected appears in the Selected pane. Click **Next**.



7. Read the confirmation screen, and then click **Finish**. VCM Patching creates your template and places it in the Assessment Templates folder (**Patching | Windows | Assessment Templates**).

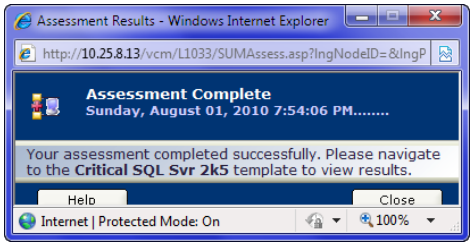
Run the Assessment

To complete the VCM Patching assessment, you must run the template that you just created.

IMPORTANT VCM PatchingAssessments are run against the data from every VCM-managed Windows machine in the active Machine Group. However, patches can only be deployed to machines managed by VCM Patching.

To run the assessment template, follow these steps.

1. Verify that the correct Machine Group is active.
2. Click **Patching | Windows | Assessment Templates**.
3. In the list of available templates, select the template that you want to run.
4. Click **Assess**. VCM displays a dialog box indicating the assessment status.


Assessment Results - Windows Internet Explorer
http://10.25.8.13/vcm/L1033/SUMAssess.asp?lngNodeID=&lngP
Assessment Complete
Sunday, August 01, 2010 7:54:06 PM.....
Your assessment completed successfully. Please navigate to the Critical SQL Svr 2k5 template to view results.
Help
Close
Internet | Protected Mode: On
100%

5. When the Assessment finishes, click the **Refresh** toolbar button and view your results.

Explore VCM Patching Windows Assessment Results

To view the assessment results on Windows machines, follow these steps.

1. Click **Patching | Windows | Assessment Templates**, and then select the name of the template that you just ran. VCM Patching displays a summary node containing the results of your assessment. This view includes a graph illustrating the patch status of the machines that you assessed, as well as additional tables listing **Patch Status by Asset Classification and Bulletin Severity Rating**. Machines that require patching, or a reboot for an applied patch, are listed in the **Not Patched** column in the Patch Status tables.
2. Click the link in this column to view a data grid containing a list of the affected machines.

Deploy Patches to Windows Machines

After running the assessment template and evaluating the results, you can deploy security patches on Windows machines that are managed by VCM Patching.

To view a data grid containing your VCM Patching-managed machines, click **Patching | VCM Patching Administration | Windows | Machines Manager | Licensed Machines**.

NOTE VMware recommends that you evaluate each patch on a case-by-case basis prior to deployment. Test the patches in a pre-production setting to verify that they work successfully within your specific environment.

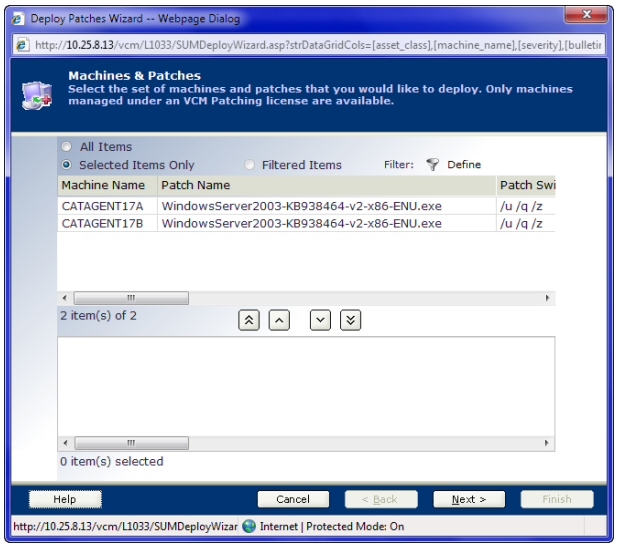
When patching Windows 2008 servers and Windows 7 machines, the Windows Update service must be running for the patch deployment to succeed. Before you begin the patch deployment, ensure that the Windows Update service is running (set to something other than "Disabled"). Otherwise, the patch deployment job will fail.

After completing the assessment, follow these steps to deploy patches to Windows machines.

1. Click **Patching | Windows | Assessment Templates**, and then select the name of the template from which you want to deploy a patch.
2. Click **View Data Grid** to view the tabular representation of the affected machines.
3. Select the row or rows showing the machines to be patched.
4. Click **Deploy**. VCM Patching displays the **Deploy Patches** wizard. For information about setting the

patch staging, deployment, and reboot options, see Patch Staging and Deployment Schedule in the online Help.

NOTE If you have a licensed VCM Service Desk Integration implementation, the Service Desk Connector dialog will appear prior to the VCM Patching Deploy Patches Wizard. For more information about VCM Service Desk Integration, see Getting Started with Service Desk Integration.



5. Select the machines and patches that you want to deploy, and then click **Next**. The **Deploy Wizard** attempts to detect the patch or patches in the following order:
   - On the Collector, the **Deploy Wizard** uses a previous download of the patch or patches.
   - If the patches are not found on the Collector, the **Deploy Wizard** will attempt to locate the patch or patches through the Internet.

   If access to the Internet is denied, locate the patches manually and save them to the \\collector_name\cmfiles$\SUM Downloads directory on your Collector machine.

NOTE If the patch or patches are found on the Internet, you must select one of the following options:
Download at run time: Downloads the patch as part of the deploy job.
Download now: Downloads the patch separately from the deploy job.

---

6. Click **Next**.
7. Confirm the patches to include in the deployment, and then click **Next**.
8. Click **Next** to either schedule the deploy job or to instruct VCM Patching to execute the job immediately. If you have licensed and activated VCM Service Desk Integration, the deploy job must be approved through VCM Orchestrator before it can run.
9. Click **Finish** to complete the deploy job.

NOTE Navigate to **Patching | VCM Patching Administration | Windows | Job Manager | Running** to view the status of your job. If you have scheduled the job to run later, navigate to **Patching | VCM Patching Administration | Windows | Job Manager | Scheduled | Deployments**.

If you have licensed and activated VCM Service Desk Integration, your Windows patching job will appear in the Pending Response node until it is approved by VCM Service Desk Connector. For more information about VCM Service Desk Integration, seeGetting Started with Service Desk Integration.

When the deployment completes, VCM Patching automatically runs a delta collection of the VCM Patching Security Bulletins filter set so that the assessment information is up-to-date.

10. As a final verification step, VMware recommends that you run a post-deployment assessment to verify that the patches you deployed are now marked as **Patched** in the node summary.

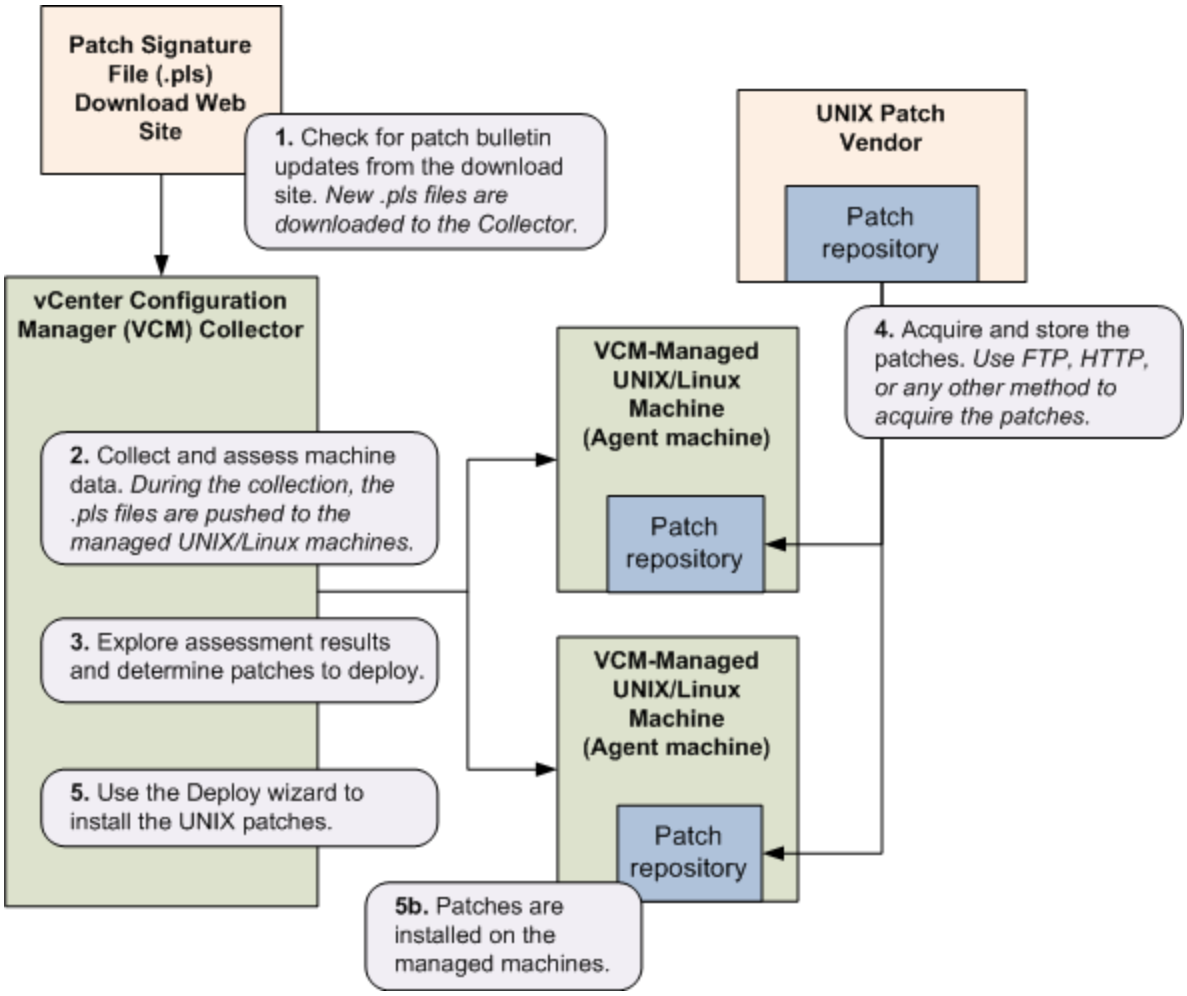
NOTE If the machine is in a pending reboot state, the machine is displayed as Not Patched.

IMPORTANT At any point, if a failure occurs in the patch deployment job, the System Administrator should check the status of the system, resolve any issues as necessary, and then reassess.

For information about scheduled deployments for Windows machines, see the online Help.

Getting Started with VCM Patching for UNIX/Linux Machines

Welcome to VCM Patching for UNIX/Linux. When licensed, you can use VCM Patching for UNIX/Linux to determine the patch status of UNIX/Linux machines. The process is as follows:


Patch Signature File (.pls) Download Web Site
1. Check for patch bulletin updates from the download site. New .pls files are downloaded to the Collector.
UNIX Patch Vendor
Patch repository
vCenter Configuration Manager (VCM) Collector
4. Acquire and store the patches. Use FTP, HTTP, or any other method to acquire the patches.
VCM-Managed UNIX/Linux Machine (Agent machine)
2. Collect and assess machine data. During the collection, the .pls files are pushed to the managed UNIX/Linux machines.
Patch repository
3. Explore assessment results and determine patches to deploy.
VCM-Managed UNIX/Linux Machine (Agent machine)
5. Use the Deploy wizard to install the UNIX patches.
Patch repository
5b. Patches are installed on the managed machines.

As indicated in this diagram, you must always collect assessment data from the UNIX/Linux machines before using VCM Patching to install the patches on them.

NOTE Assessments of UNIX/Linux-based machines operate differently from Windows assessments: UNIX assessments require new data to be collected, while Windows assessments are performed against previously collected data.

Getting Started

To get started, follow these steps:

Step 1: Check for updates to bulletins.

Step 2: Collect assessment data.

Step 3: Explore the results, and acquire and store the patches.

Step 4: Install the patches.

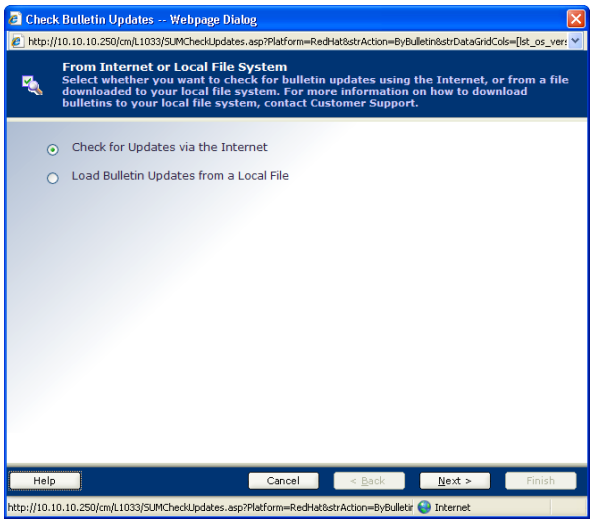
NOTE Before you can deploy patches to a UNIX/Linux machine, VCM Patching for UNIX must be licensed on the UNIX/Linux machine.

For a list of UNIX/Linux machines and operating systems supported for patch deployment, see the *VCM Hardware and Software Requirements Guide*.

Check for Updates to Bulletins

VMware recommends that you use VCM to check for updates to VCM Patching Bulletins prior to performing an assessment for UNIX/Linux machines. To check for updates to VCM Patching Bulletins, follow these steps.

1. Click **Patching | [UNIX/Linux Platform] | Bulletins | By Bulletin**.
2. Click **Check for Update** in the data grid tool bar.
3. VCM Patching displays a dialog box communicating the status of your request. Follow the prompts to check for updates to bulletins.


Check Bulletin Updates -- Webpage Dialog
From Internet or Local File System
Select whether you want to check for bulletin updates using the Internet, or from a file downloaded to your local file system. For more information on how to download bulletins to your local file system, contact Customer Support.
Check for Updates via the Internet
Load Bulletin Updates from a Local File
Help
Cancel
< Back
Next >
Finish
Internet

Collect Assessment Data from UNIX/Linux Machines

You can collect UNIX/Linux assessment data in several ways:

- Using Bulletins
- Using a Template
- Using the Collect Wizard

The assessments must complete successfully before you can install patches. If a patch assessment does not return any results, see the troubleshooting section.

To filter the assessment data, see Creating UNIX/Linux Patch Assessment Filters in the online Help.

NOTE UNIX/Linux patch assessments are based on the OS version and machine architecture. When using templates to collect UNIX/Linux assessment data, pay close attention to the title of the bulletins to ensure that you are specifying 32-bit or 64-bit bulletins in your template.

Prerequisites for Assessment

Before assessing the VCM-managed machines:

- The Patch Signature File (.pls) files must reside on the Collector. By default, VCM Patching is set to execute the action to download the .pls files automatically every 4 hours. The .pls files are used to determine if required patches are installed on the VCM-managed machine. You can view the patch files in: **Console | UNIX | Security | Patches | Assessment** or **Console | Change Management | Non VCM Initiated | By Machine**. During a patch assessment, using the Patch Assessment data type, the .pls files are pushed from the Collector to the VCM-managed machine. You may experience a delay while this process is occurring.
- The VCM Agent must be installed on the VCM-managed machine.
- The VCM-managed machine must be licensed for VCM Patching for UNIX Patching.

NOTE Assessments of UNIX/Linux-based machines operate differently from Windows assessments: UNIX assessments require new data to be collected, while Windows assessments are performed against previously collected data.

Machine Assessments are Run Against Known Patches

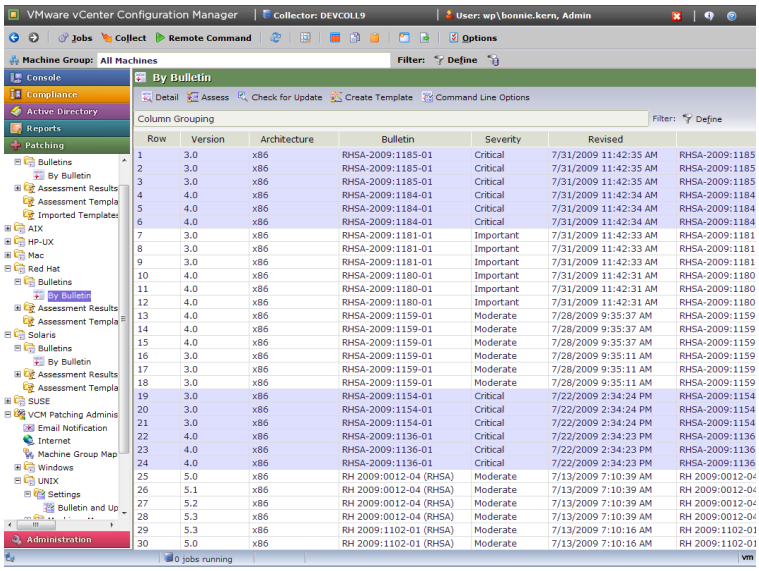
Assessments of UNIX/Linux machines are run against the patches known by VMware at the time the assessment is performed. For more information, contact VMware Customer Support.

NOTE If machine data has not been collected for a machine, VCM Patching may not display assessment results for the machine, and the machine will not be available for deployment. In cases where a patch-machine mismatch occurs, VCM can be set to display the data and the mismatch status, or hide the patch-machine mismatch data in **Patching | VCM Patching Administration | UNIX | Settings | Bulletin and Update**.

Using Bulletins to Run an Assessment

To run an assessment using bulletins, follow these steps.

1. Click **Patching | [UNIX/Linux Platform] | Bulletins | By Bulletin**.



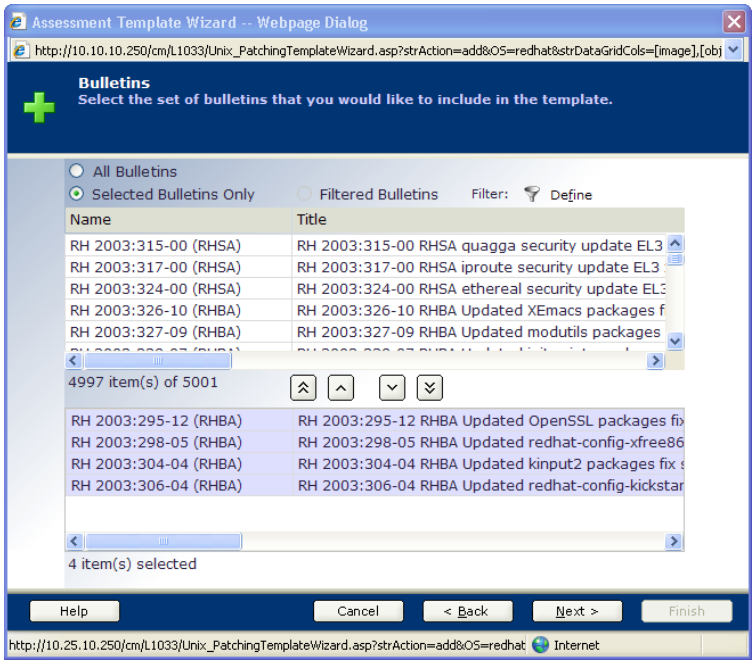
2. Click **Assess**. The assessment on UNIX/Linux machines uses the **Patch Assessment** collection filter to perform a collection of all machines in the current machine group. The results are reported in the

Assessment Results node.

Using a Template to Run an Assessment

UNIX assessment templates are filters for the patch assessment results data. To run an assessment and filter the assessment data using a template, follow these steps to create and run an assessment template:

1. Click **Patching**, and then click the **UNIX/Linux Platform** of your choice.
2. Click **Assessment Templates**.
3. Click **Add**, and then add Bulletins to your assessment template.



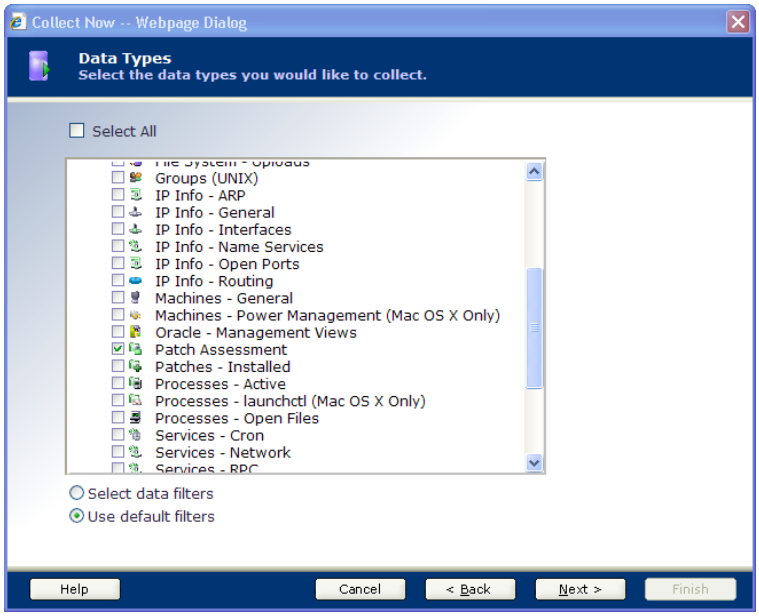
4. Complete the wizard to build your assessment template.
5. In the **Assessment Templates** navigation pane, select the new template and view the data grid.
6. In the data grid for the template, click **Assess**. The assessment on UNIX/Linux machines uses the **Patch Assessment Data Class** filter to perform a collection of all machines in the current machine group. When the assessment completes, the results are reported in the **Assessment Results** node.

Using the Collect Wizard to Run an Assessment

When assessing UNIX/Linux machines, clicking **Collect** allows you to specify individual machines for the assessment. To assess UNIX/Linux machines using the **Collect** wizard, follow these steps.

1. Click **Collect** in the toolbar. The **Collection Type Selection** wizard appears.

2. Follow the **Collect** wizard and select the option to collect machine data. Specify the UNIX machines to collect data from, specify a data type to use for the collection, and then select the **Patch Assessment** data type. Alternatively, you could collect using the **UNIX Patch Assessment** collection filter.



3. Complete the wizard. When the assessment completes, the results are reported in the **Assessment Results** node.

Scheduling UNIX/Linux Assessments

Because UNIX/Linux assessments are VCM collections, you can schedule these assessments by using the **Patch Assessment** collection filter.

Patching Change Actions are Saved in the VCM Change Log

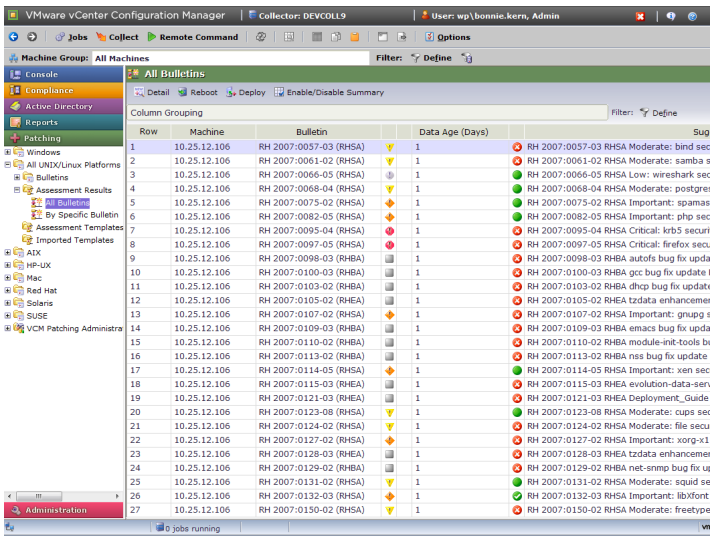
UNIX/Linux patching change actions are saved in the VCM change log in **Console | Change Management | VCM or Non VCM Initiated Change | By Data Type | Patch Assessment**. These change actions are also available to Compliance and Reports.

Explore Assessment Results and Acquire the Patches

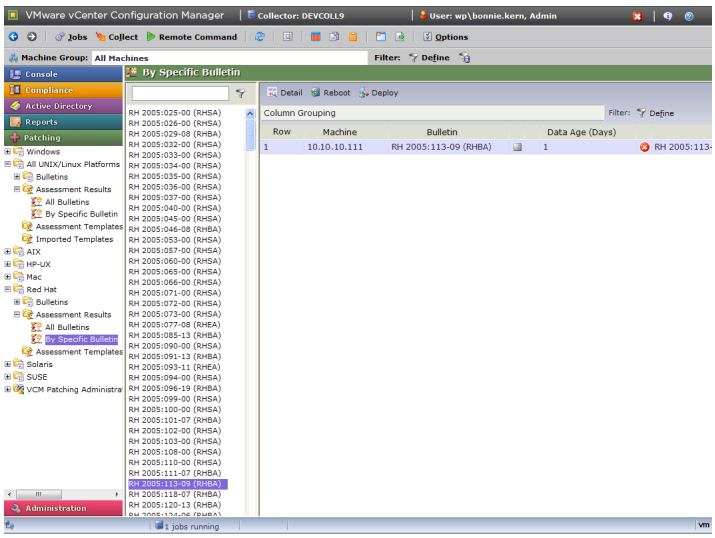
After you have collected assessment data from your VCM-managed UNIX/Linux machines, use the **Assessment Results** data grid to view the assessment results. This data grid displays all of the UNIX/Linux machines that were assessed, the patch status for each machine, and details about the patches.

In **Patching | [UNIX/Linux Platform] | Assessment Results**, follow these steps to view the results.

1. Click **All Bulletins** to display the **Patch Assessment Results** for all bulletins that VCM assessed against. This view displays the patch status of all of the machines that were assessed.



2. Click **By Specific Bulletin** to display the **Patch Assessment Results** for a single bulletin. Click a bulletin number in the center pane to display the applicable patch assessment results in the data grid.



3. Review the patch status for each machine. The patch status for the assessed machine is indicated by one of the following icons:

Patch Status	Description
	Patched: The patch has already been applied to this UNIX/Linux machine.
	Patch-Machine Mismatch: The operating system version or hardware architecture of the patch do not match those of the UNIX/Linux machine.
	Patch Not Needed: The machine is already up-to-date, or the application that the patch is intended to fix is not installed on the machine.
	Not Patched: The patch has not been applied to this UNIX/Linux machine.
	Error Occurred: Indicates that an unexpected condition occurred during the assessment processing on the UNIX/Linux machine. For potential additional information about the root cause of the exception, run the Debug Event Viewer (C:\Program Files\VMware\VCM\Tools\ecmDebugEventViewer.exe).
	Signature Not Found: The .pls patch file is not found on the UNIX/Linux machine, and therefore the patch status cannot be determined for the particular .pls file.
	Incorrect MD5: The MD5 Hash generated from the patch file (.pls), which contains the content and signature, does not match the expected value on the UNIX/Linux Agent. (Note that MD5 is NOT validated against the vendor MD5 hash data.)
	Patch Status Unknown: The machine's patch status cannot be determined.

NOTE If machine data has not been collected for a machine, VCM Patching may not display assessment results for the machine, and the machine will not be available for deployment. In cases where a patch-machine mismatch occurs, VCM can be set to display the data and the mismatch status, or hide the patch-machine mismatch data in **Patching | VCM Patching Administration | UNIX | Settings | Bulletin and Update**.

Acquiring the UNIX Patches

After reviewing the assessment results and determining which patches to deploy, acquire the UNIX patches yourself from the appropriate vendor using FTP, HTTP, or any other method available to you.

Storing the UNIX Patches

Store the UNIX patches in a location that is available locally to the VCM-managed machine, such as an NFS mount or a local hard drive. If you store the patches on an NFS mount, you must define the path in **Patching | VCM Patching Administration | Machine Group Mapping**.

You can use VCM remote commands or another method available to you to get the patches to the VCM-managed machines.

Patch Repository Management

You must manage your own patch repository. A temporary expansion of the patches will be performed in the `/tmp` directory. For single-user mode, patches are extracted to `/var/tmp`. If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` will be used.

Machine Group Mapping

If you define an alternate location for a particular Machine Group such as Servers (in **Patching | VCM Patching Administration | Machine Group Mapping wizard | Local Patch Path**), you must select that Machine Group at the top of the VCM Portal before you deploy the patches. Otherwise, if the same Machine Group is not selected, VCM Patching will not acknowledge the machine group mapping to the alternate patch location, and the patches will not be deployed.

Default Location for UNIX/Linux Patches

If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` will be used. A temporary expansion of the patches will be performed in the `/tmp` directory.

Deploy Patches to UNIX/Linux Machines

After running the assessment template and evaluating the results, and acquiring and storing the patches, you can install the patches on the UNIX/Linux machines that are managed by VCM Patching. The deploy action assesses whether the patch was installed on the VCM-managed machine.

For a list of UNIX/Linux machines and operating systems supported for patch deployment, see the *VCM Hardware and Software Requirements Guide*.

Prerequisites for Deployment

Before deploying the patches to VCM-managed UNIX/Linux machines, ensure the following:

- VCM Patching for UNIX must be licensed on the UNIX/Linux machine.
- Ensure that the assessments have run successfully.
- The patches must be available locally to the VCM-managed machine.

IMPORTANT **If you will be deploying patches in single-user mode on UNIX machines, you MUST do the following:**

1) Store or extract the patches in a local location other than `/tmp` that will be accessible in single user-mode.
2) If you did not manually extract the files in step 1, ensure enough disk space exists to extract the patches in `/var/tmp`.
3) Set the machine group mapping to the patch path location where you have stored the patches.

If you will be deploying patches without changing the run level, you must do the following:

1) Store or extract the patches in a local location (not /tmp on Solaris as this directory will be cleaned out upon reboots that may be initiated by the patches).
2) If you did not manually extract the files in step 1, ensure enough disk space exists to extract the patches in `/tmp` (or `/var/tmp` on Solaris).
3) Set the machine group mapping to the patch path location where you have stored the patches.

Default Location for UNIX/Linux Patches

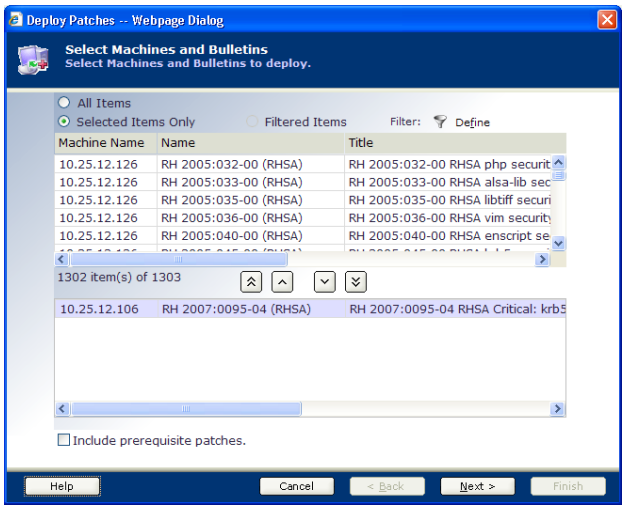
If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` will be used. A temporary expansion of the patches will be performed in the `/tmp` directory.

Deploying the Patches

NOTE Before deploying patches, see Patch Deployment Notes in the online Help.

You can install the UNIX patches using the **Deploy** wizard from the following locations: **User-created Assessment Template**, **Imported Template**, or **Assessment Results (All Bulletins)**. To install the patches on UNIX/Linux machines, follow these steps; this example shows deploying the patches using **All Bulletins**.

1. After acquiring and storing the patches, select the patches by clicking **Patching | [UNIX/Linux platform] | Assessment Results | All Bulletins**.
2. View the **All Bulletins** data grid, and then select the patches you want to deploy.
3. To deploy one or more patches, click **Deploy**, and then complete the wizard. VCM performs another collection so you can confirm that the patches were applied.



For more information about other ways to deploy patches, see Using the Deployment Wizards in the online Help.

Patching Change Actions are Saved in the VCM Change Log

UNIX/Linux patching change actions are saved in the VCM change log in **Console | Change Management | VCM or Non VCM Initiated Change | By Data Type | Patch Assessment**. These change actions are also available to Compliance and Reports.

IMPORTANT At any point, if a failure occurs in the patch deployment job, the System Administrator should check the status of the system, resolve any issues as necessary, and then reassess.

How the Deploy Action Works

The **Deploy** action (**Deploy** wizard) runs a command from the Collector to the VCM-managed machines. The VCM job command performs the following actions:

- Assesses VCM-managed machines to determine whether the patch has been installed since the last assessment.
- Runs a pre-install script (remote command) if specified (see note below).
- Installs the patch that already resides on the VCM-managed machine's NFS mounted or local file system.
- Runs a post-install script (remote command) if specified (see note below).
- Assesses whether the patch was installed on the VCM-managed machine.

The pre-install and post-install scripts used in the **Deploy** actions are remote commands, which differ from using a VCM remote command to install a patch. The patch assessment and deployment process for UNIX/Linux does not use remote commands. However, if you choose to deploy a patch using a user-created remote command, be aware that the patch will not be assessed until you run an assessment.

Further Reading

Refer to Customizing VCM for information on how to customize for your environment. Several of these areas regarding customization also apply to VCM Patching. Also read Maintaining VCM after Installation for important information regarding additional data retention settings and database maintenance steps that should be taken.

While using VCM Patching, refer to the online Help for specific information.

Getting Started with Software Provisioning 9

The VCM Software Provisioning components consist of VMware vCenter Configuration Manager Package Studio, software package repositories, and Package Manager.

VMware vCenter Configuration Manager Package Studio

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

A software package provides the files and metadata necessary to install and remove programs. One of the most useful features of a package is the metadata regarding dependencies, conflicts, and other relationships that are not represented by software installation files. This metadata is used to determine if the necessary dependencies are in place so that an installation is successful, and if not, what is necessary to make the installation successful. This use of metadata is similar to rpm on Linux.

Packages support commercial and custom software that may be installed using any installation technology, including .msi, .exe, or scripts (Python, VBScript, PowerShell, and others).

Once a package is created and ready for distribution, it is published to a software repository. You use Package Manager to download the package from the repository to the local machine and install it on your Windows systems.

Software Repository for Windows

Software Repository for Windows is the shared location to which packages are published by Package Studio and the location from which Package Manager downloads packages for installation.

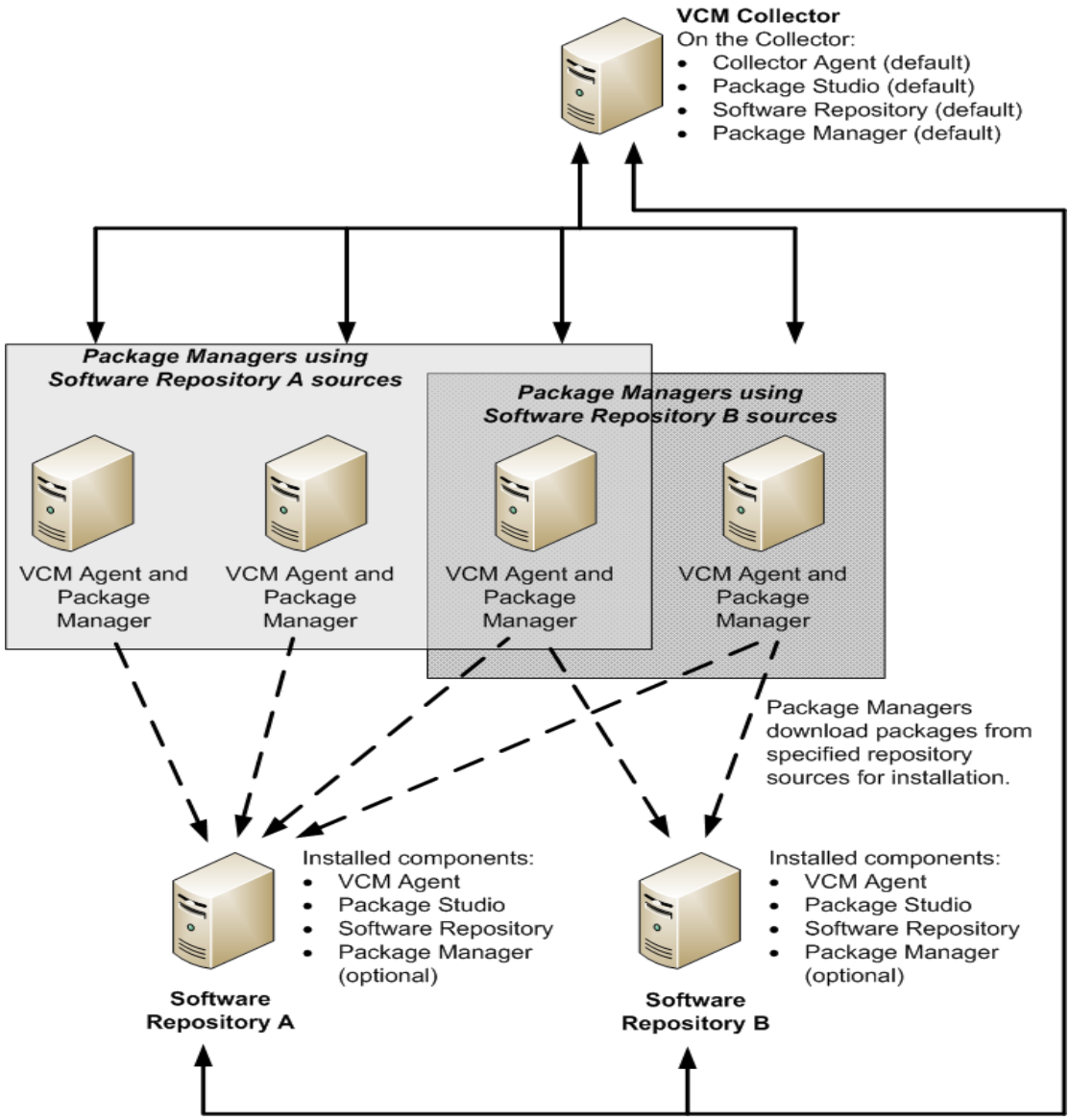
Package Manager for Windows

Package Manager is the application installed on each machine to manage the installation and removal of the software contained in packages. Package Manager is configured to use one or more repositories as sources for packages.

If you are using the software provisioning components in conjunction with VMware vCenter Configuration Manager (VCM), you can use VCM to add and remove sources, and to install and remove packages.

Overview of Component Relationships

The following diagram displays the general relationship between Package Studio, repositories, and Package Manager in a working environment.



Installing the Software Provisioning Components

The software provisioning components should be installed on machines with the following relationships:

NOTE By default, all the components are installed on the VCM Collector; however, it is recommended you use a separate machine for the Software Repository for Windows and the **VMware vCenter Configuration Manager Package Studio**.

- **Software Repository for Windows:** Installed on at least one Windows machine in your environment, and installed on the same machine with Package Studio. Install the repository before installing Package Studio.
- **VMware vCenter Configuration Manager Package Studio:** Installed on the same machine as your software repository.
- **Package Manager:** Installed on all Windows machines on which you are managing software provisioning.

To uninstall the above applications using a script at a later date, you should save a copy of each of the .msi files in an archive location. To uninstall using the .msi, you must have the same version used to install the application.

Install Software Repository for Windows

The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. The process installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

Prerequisites

Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.

Access to the Repository.msi, which is available on the VMware website or in the vCenter Configuration Manager application files.The default location in the VCM application files is `C:\Program Files\VMware\VCM\AgentFiles\Products`.

Procedure

1. Double-click `Repository.msi`.

   The **Welcome** page appears.

2. Click **Next**.

   The **License Agreement** page appears.

3. Review the agreement, and then select **I accept the terms of the License Agreement** to continue. The other options become available.

4. Select **I am an authorized agent and/or representative of the customer/end-user** and **I have read the terms and conditions stated above**.

5. Click **Next**.

   The **Installation Folder** page appears.

6. Use the default path or click **Change** to modify the path. When the path is correct, click **Next**.

   The **Virtual Directory** page appears.

7. Use the default name or type a new name in the text box.

8. Click **Next.**

   The **Ready to Install** page appears.

9. Click **Install**.

   When the installation is completed, the **Setup Complete** page appears.

10. Click **Finish**.

The repository and the virtual directory are added to the locations specified during installation. The default location for the repository is `C:\Program Files\VMware\VCM\Tools\Repository` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Repository` (on 64-bit machines). The default virtual directory SoftwareRepository is added to **Internet Information Services (IIS) | Web Sites | Default Web Site**.

Procedure (unattended using .msi)

1. On your Collector, navigate to `C:\Program Files\VMware\VCM\AgentFiles\Products.`
2. Locate the `Repository.msi` file, and then copy it to the target machine. You can also run it from a shared location.
3. On the target machine, run the .msi file using the following command line syntax.

   ```
   msiexec /i [path]\Repository.msi /qn /l*v %temp%\Repository.log
   ```

   You can add the following arguments if you want to specify locations other than the default directories:

   REPOSITORY_ROOT="C:\Program Files\VMware\VCM\Tools\Repository\" (defaults to this path)

   VIRTUAL_DIR_NAME_REPOSITORY=SoftwareRepository (defaults to this value)

Software Repository Structure

The files for a repository consist of the main folder (for example, SoftwareRepository). In this file are the following:

- .hive: Contains the repository management files, including such files as repository.index and repository.toc.
- crates: Contains alphabetical sub folders. It is to this location that the packages (.crate files) are published.
- dists: Contains crates.gz files. These files are metadata about the .crate files.

Manually Uninstall the Repository

Use the following script to run an unattended uninstall the software repository. To uninstall the application, you must use the version of the Repository.msi that was used to install the application.

Procedure

1. Copy the Repository.msi to the machine on which you are uninstalling the application or point to the file in a shared directory.
2. Run the .msi file using the following command line syntax:

   ```
   msiexec /x [path]\Repository.msi /l*v %temp%\Repository.log
   ```

Install Package Studio

The VMware vCenter Configuration Manager Package Studio and the repository must be installed on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

NOTE When Package Studio is uninstalled from a machine, the locally saved projects and .crate files remain on the machine, allowing you to copy them to another machine or to delete them manually if they are not needed.

Prerequisites

Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.

Access to the PackageStudio.msi, which is available on the VMware website or in the vCenter Configuration Manager application files. The default location in the VCM application files is C:\Program Files\VMware\VCM\AgentFiles\Products.

(Recommended) Software Repository for Windows is installed. Installing the repository before installing Package Studio will reduce the manual configuration steps.

Procedure

1. Double-click `PackageStudio.msi`.

   The **Welcome** page appears.

2. Click **Next**.

   The **License Agreement** page appears.

3. Review the agreement, and then select **I accept the terms of the License Agreement** to continue. The other options become available.

4. Select **I am an authorized agent and/or representative of the customer/end-user** and **I have read the terms and conditions stated above**.

5. Click **Next**.

   The **Installation Folder** page appears.

6. Use the default path or click **Change** to modify the path. When the path is correct, click **Next**.

   The **Repository Root Folder** page appears.

7. Verify the path is to your installed repository files. To modify, click **Change**. When the path is correct, click **Next**.

   The **Ready to Install** page appears.

8. Click **Install**.

   When the installation is completed, the **Setup Complete** page appears.

9. Click **Finish**.

The Package Studio is installed to the location specified during installation. The default location is `C:\Program Files\VMware\VCM\Tools\Package Studio` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Package Studio` (on 64-bit machines). To start Package Studio, select **Start | All Programs | VMware vCenter Configuration Manager | Tools | Package Studio**, or open the Package Studio folder and double-click **PackageStudio.exe**.

Procedure (unattended using .msi)

1. On your Collector, navigate to `C:\Program Files\VMware\VCM\AgentFiles\Products`.

2. Locate the `PackageStudio.msi` file, and then copy it to the target machine. You can also run it from a shared location.

3. On the target machine, run the .msi file using the following command line syntax.

   ```
   msiexec /i [path]\PackageStudio.msi /qn /l*v %temp%\PackageStudio.log
   ```

You can add the following arguments if you want to specify locations other than the default directories:

REPOSITORY_ROOT=C:\Program Files\VMware\VCM\Tools\Repository\ (Defaults to this or uses the Repository's value if it is already installed)

PACKAGESTUDIO_DIR="C:\Program Files\VMware\VCM\Tools\Package Studio\" (defaults to this path)

Manually Uninstall Package Studio

Use the following script to run an unattended uninstall the Package Manager. To uninstall the application, you must use the version of the PackageStudio.msi that was used to install the application.

Procedure

1. Copy the PackageStudio.msi to the machine on which you are uninstalling the application. You can also run it from a shared location.
2. Run the .msi file using the following command line syntax:

```
msiexec /x [path]\PackageStudio.msi /l*v %temp%\PackageStudio.log
```

Install Package Manager on Managed Machines

The Package Manager is automatically installed on target machines when the 5.3 VCM Agent is installed.

On the target machine, the Package Manager does not contain the software packages, only pointers to the packages in the repository sources of which it is aware. When directed to install, the package is copied from the repository to the cratecache folder on the target machines. It is from this location that Package Manager upzips the files to the %TMP% directory and runs the configured installation.

When a Remove Package action is sent to Package Manager, it checks first for the package in the cratecache. If it is not found, it then checks the repository sources for the package, and again copies it to the target machine's cratecache folder. It is from this location that it unzips the files. The configured uninstall files may be run form the zip directory.

Installing the VCM Agent

If you are preparing to use software provisioning on machines not previously managed in VCM, you must first install the VCM Agent. See "Installing the VCM Windows Agent on your Windows Machines" on page 61 for complete instructions. By default, the VCM Agent installation installs the agent extensions for provisioning and the Package Manager for Windows. This default action is based on the settings in **Administration | Settings | General Settings | Installer**.

Prerequisite

Target machine meets the supported hardware requirements, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.

Verifying the Installation of the Agent Extensions for Provisioning

If you do not know if the machines are ready to use provisioning or not, you can verify the version of the Agent Extensions for Provisioning. The Agent Extensions for Provisioning include the Package Manager.

1. Select **Administration | Machines Manager | Licensed Machines | Licensed Windows Machines**.
2. In the data grid, locate the machines on which you are verifying the existence of the necessary Agent Extensions, and then verify that the Agent Ext. For Prov. Version column contains a value of 5.3 or later. If it does not, you need to either install or upgrade the VCM Agent.

Upgrading the VCM Agent

If an earlier VCM Agent is installed on your machines, you will need to upgrade to the latest Agent. See Upgrade Agent in the online Help.

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Creating Packages

A software package provides the files and metadata necessary to install and remove programs. One of the most useful features of a package is the metadata regarding dependencies, conflicts, and other relationships that are not represented by software installation files. This metadata is used to determine if the necessary dependencies are in place so that an installation is successful, and if not, what is necessary to make the installation successful. This use of metadata is similar to rpm on Linux.

Packages support commercial and custom software that may be installed using any installation technology, including .msi, .exe, or scripts (Python, VBScript, PowerShell, and others).

Once a package is created and ready for distribution, it is published to a software repository. You use Package Manager to download the package from the repository to the local machine and install it on your Windows systems.

Creating a software package includes creating and saving a project. Projects can be used to create variations based on platform or version that can then be published as separate packages.

General Process

Detailed steps for creating and publishing packages are provided in the Package Studio online Help and in the *VCM Software Provisioning Installation and User's Guide*.

1. Start the VMware vCenter Configuration Manager Package Studio. Select **Start | All Programs All | VMware vCenter Configuration Manager | Tools | Package Studio**.
2. Click **Manage Packages**. Configure the package contents based on the options on the following tabs:
   a. Click **Properties**. Type a **Name**, **Version**, and **Description**. Select the **Architecture**. These are required fields. You have the option to update the other fields, depending on you requirements.

      Configuring the package with Depends, Conflicts, Provides, and adding and configuring the installation and removal files.

   b. Click **Files**. Import the installation files, add pre-command files, configure the commands and arguments, and add post-command files.
   c. Click **Save** to save the setting and files as a Project (*.prj).
   d. Click **Generate** to save the project as a package (*.crate).
3. Click **Package Signing**. Sign the package with a signing certificate.
   a. Click **Open** to select a package (*.crate file).
   b. Click **Sign**. Select a certificate from the certificate store or from a file.
4. Click **Manage Repositories**. Select the platforms and sections to which you are publishing the package.
   a. Click **Add Platforms** to add a platform.
   b. Select a platform, and then click **Add Sections**.
   c. Select a section, and then click **Publish Package**.
   d. Select the package (.crate), and then click **Open**. The **Publish Package** dialog box appears.
   e. (Optional) Select additional platforms and sections to which to publish the package.
   f. Click **Publish**. The package is published to the software repository.
5. Click **External Software**. Add externally managed software, especially any packages specified as depends or conflicts in any of your packages.
   a. Click **New External Package** and replace the text with the name you will use as an external software package name.
   b. Type a version number in the **Version** text box.
   c. Select the **Architecture** in the drop-down list.
   d. Click **Select Attribute Name** and select a registry property or WMI attribute in the drop-down list.
   e. Add attributes.
   f. To save a copy locally, click **Save** .
   g. Click **Publish External SW** to publish to the repository.

Using VCM Software Provisioning for Windows

Using VCM Software Provisioning, you can collect and view Repository and Package Manager data, and then install, update, or remove packages.

Prerequisites

The following prerequisites must be met before you can begin using VCM Software Provisioning:

- You have created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories.
- Package Manager is installed on the target machines. Package Manager is automatically installed when you install the VCM 5.3 Agent or later.

Collect Package Manager Information from Machines

To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

As you work with provisioning, you will want to regularly collect Package Manager data to determine if your machines are remaining current with the necessary software packages.

Procedure

1. Click **Collect**.

   The **Collection Type** page of the **Collection Wizard** appears.
2. Select **Machine Data**.
3. Click **OK**. The **Machines** page appears.
4. Verify that the **Selected** pane displays all the machines from which you are collecting package manager data. Add any machines as needed.
5. Click **Next**. The **Data Types** pages appears.
6. Expand **Windows**, and then select **Software Provisioning - Package Managers**.
7. Click **Next**. The **Important** page appears.
8. Review the information, resolve any conflicts, and then click **Finish**. You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 190 for more information.

When the collection is completed, select **Console | Windows tab | Operating System |Software Provisioning | Package Managers**. The data grid displays the packages and their current status.

Collect Software Repository Data

A collection of repository data will include the software packages in the repository, allowing you to determine which repositories to assign to machines based on the available packages.

TIP Create a Machine Group containing all machines on which the software repository is installed.

Procedure

1. Click **Collect**.

   The **Collection Type** page of the **Collection Wizard** appears.
2. Select **Machine Data**.
3. Click **OK**. The **Machines** page appears.
4. Verify that the **Selected** pane displays all the machines from which you are collecting repository data. Add any machines as needed.
5. Click **Next**. The **Data Types** pages appears.
6. Expand **Windows**, and then select **Software Provisioning - Repositories**.
7. Click **Next**. The **Important** page appears.

8. Review the information, resolve any conflicts, and then click **Finish**. You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 190 for more information.

When the collection is completed, select **Console | Windows tab | Operating System |Software Provisioning | Repositories**. The data grid displays the packages in the repositories.

Add Repository Sources to Package Managers

Sources are the sections in the repository from which the Package Manager will be able to download and install packages.

Adding a source gives the Package Manager on the selected machines access to the packages available in specified section. The sources are numbered in priority order. When you add a new one, you can specify whether to add it to the beginning or to the end of the list. You can also remove sources.

Procedure

1. Select **Console | Windows tab | Operating System |Software Provisioning | Package Managers** data grid.
2. Select one or more machines, and then click **Add Source**.

   The **Select Machines** page of the **Add Source** wizard appears.
3. Verify that the machines displayed in the lower pane are the machines to which you want to add the source. Add or remove machines as needed.
4. Click **Next**.

   The **Enter or Select Source** page appears.
5. Select either **Add source at the beginning of existing source lists** or **Add source at the end of the existing source list**.
6. Type the **URI** or click **Browse Sources**. If you click **Browse Sources**, the **Browse Sources** page appears. In the Show Sources from drop-down list, select one of the following:
   - **Package Manager Source Lists:** Select this option if you have already added sources to at least one Package Manager and you want to add the source to other Package Managers. When you click **OK**, the selected source automatically populates the **Platform** and **Section** field on the **Enter or Select Source** page.
   - **VCM Managed Repositories:** Select this option if the source has not yet been added to a Package Manager. When you return to the **Enter or Select Source** page, you must type the platform and section names in the appropriate text boxes.
7. Type a **Platform** name and a **Section** name. The names must be typed exactly as they are used in the repository.
8. Click **Next**.

   The **Schedule** page appears.
9. Select one of the scheduling options and configure as needed.
10. Click **Next**.

    The **Confirmation** page appears.
11. Review the information. If it is correct, click **Finish**.

    You can monitor the status of the process using **Jobs Manager | Running**.

The added source is displayed in the **Package Manager - Sources** data grid.

Install Packages

The process of installing packages includes identifying and processing dependencies and conflicts, running any specified prescripts, running the installation using any specified command arguments, and then running any specified post-scripts. You can also remove packages.

Procedure

1. Select **Console | Windows tab | Operating System |Software Provisioning | Package Managers**
2. Click **Install**.

   The **Select Machines** page of the **Install Package** wizard appears.
3. Verify that the machines displayed in the lower pane are the machines to which you want to install the package. Add or remove machines as needed.
4. Click **Next**.

   The **Select Package** to Install page appears.
5. In the **Package Name** list, select the package to install.
6. Select one of the following version options:
   - **Install Version:** Installs the specified version. By default the operator equals the package selected in the list; however, you may select a different operator and type the version number in the text box.
   - **Install latest available version on all platforms:** Installs the latest version of the package available from the sources configured for the Package Manager.
7. Configure the **Security Options**.

   This option determines if a package is installed or removed based on the state of the signature. Select one of the following options:
   - **Install secure signed package only:** The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.
   - **Skip signature validation when installing a signed package:** (Not Recommended) The package is installed or removed without attempting to verify the signature.
   - **Allow unsigned package to be installed:** (Not recommended) The package is installed or removed even if it is unsigned.
8. Click **Next**.

   The **Schedule** page appears.
9. Select one of the scheduling options and configure as needed
10. Click **Next**.

    The **Confirmation** page appears.
11. Review the information. If it is correct, click **Finish**.
12. Review the information, resolve any conflicts, and then click **Finish**. You can monitor the process in the **Jobs Manager**. See **"Viewing Provisioning Jobs in the Job Manager" on page 190** for more information.

The package is displayed as Installed in the **Package Manager - Packages** data grid.

Related Software Provisioning Actions

You can use the following management options in VCM when working with software provisioning:

- **Job Manager:** Displays current jobs running, and job history. Use the job history when troubleshooting the processing of a job. See "Viewing Provisioning Jobs in the Job Manager" on page 190 for more information.
- **Compliance:** You can create compliance rules based on software provisioning data types, and you can add provisioning remediation actions to rules.
  - "Creating Compliance Rules based on Provisioning Data" on page 190
  - "Creating Compliance Rules containing Provisioning Remediation Actions" on page 191
- **User Rules and Roles:** You can define user access rules and roles to specify what level of access users have to the Software Provisioning data and actions in VCM. Select **Administration** | **User Rules and Roles** | **User Manager** | **VCM Access** to configure the Access Rules and Roles.
- **Reports:** You can run reports on collected Software Provisioning data. Select **Reports** | **Machine Group Reports** | **Software Provisioning** to run the default reports, or you can create your own.
- **Change Management:** All Software Provisioning are available for auditing as part of Change Management. Select **Console** | **Change Management** | **VCM Initiated** or **Non VCM Initiated** to view the data.

  Software Provisioning actions are not eligible for rollback through Change Management. The undoing of any unwanted changes can be handled using Compliance enforcement remediation actions. See "Creating Compliance Rules containing Provisioning Remediation Actions" on page 191 for general information about remediation.

  Non VCM Initiated changes related to Software Provisioning include publishing packages to repositories from Package Studioand manually running command line actions in Package Manager.

Viewing Provisioning Jobs in the Job Manager

The Jobs Manager tells you the state of a currently running Provisioning job, including the success or failure of a job, either collecting data from machines or installing, updating, or removing packages from machines.

The currently running provisioning jobs are visible in the following locations:

- Jobs button, located on the portal toolbar.
- Administration slider. Select **Administration** | **Job Manager** | **Running**.

Job history is available in **Administration** | **Job Manager** | **Other Jobs**. The provisioning related job names include the following:

- Change Request: Add Source
- Change Request: Remove Source
- Change Request: Install Package
- Change Request: Remove Package

Creating Compliance Rules based on Provisioning Data

A Compliance rule based on Provisioning data can detect any packages or sources that are out of compliance. You can also configure remediation actions to bring the machines back into compliance.

In this example the Compliance rule checks whether the source, where platform=Any and section=Release, was added to selected Package Managers as a source. If not, then add the repository source to the machines where the rule fails.

Procedure

1. Select **Compliance | Machine Group Compliance | Rule Groups**. Either add a rule to an existing rule group or create a new rule group.
2. To add a rule to a Rule Group, expand your rule group, and then select **Rules**. The **Rules** data grid appears.
3. Click **Add**. The **Rule and Name** page of the **Rule Wizard** appears.
4. Type a **Name** and **Description** for your rule.
5. Click **Next**. The **Data Type** page appears.
6. Expand **Windows** and select the data type on which you are basing the rule. The data type does not need to be software based, you will later configure the software provisioning remediation. In this example, select **Services**.
7. Click **Next**. The **Rule Type for Services** page appears.
8. Select **Conditional (if/then)**, and then click **Next**. The **Conditional Data** properties for **Services** page appears.
9. In the **IF** area, click **Add**.
10. Select `Source Repository = YourRepository`.
11. Select **Must Exist**.
12. In the **THEN** area, select `Platform = Any` and `Section = Release`.
13. **Next**. The **Options** page appears.
14. Select a **Severity** in the drop-down list.
15. Select **Make available for enforcement where possible**.
16. Select **Software Provisioning action**.
17. Select **Add Source** in the drop-down list, and then click **Define Action**. The **Software Provisioning Compliance Remediation** page appears.
18. Select **Add source to the beginning of existing source list**.
19. Click **Browse Sources** to select the repository URI where the Platform=Any and Section=Release exist. The **Platform** and **Section** update with Any and Release respectively.
20. Click **OK** to close the page, and then click **Next**. The **Collection filters** page appears.
21. Select the Provisioning - Package Managers collection filter.
22. Click **Next**. The **Important** page appears.
23. Review the information, and then click **Finish** to save your rule.

When the Compliance Template is run, if the checks the target machines to determine if the repository source is added as a source. If it is not, the source is added to the machines Package Manager.

Creating Compliance Rules containing Provisioning Remediation Actions

When configuring a Compliance rule, you can configure the rule to perform a remediation based on a software provisioning action -- Install Package, Remove Package, Add Source, Remove Source.

In this example, you want to determine if a software application named XSoftware is correctly installed. If the software is installed correctly, a service named XService should be running. Configure a Compliance rule to determine if XService service is running. If it is not running, install the XSoftware package.

Procedure

1. Select **Compliance | Machine Group Compliance | Rule Groups**. Either add a rule to an existing rule group or create a new rule group.
2. To add a rule to a Rule Group, expand your rule group, and then select **Rules**. The **Rules** data grid appears.
3. Click **Add**. The **Rule and Name** page of the **Rule Wizard** appears.
4. Type a **Name** and **Description** for your rule.
5. Click **Next**. The **Data Type** page appears.
6. Expand **Windows** and select the data type on which you are basing the rule. The data type does not need to be software based, you will later configure the software provisioning remediation. In this example, select **Services**.
7. Click **Next**. The **Rule Type for Services** page appears.
8. Select **Conditional (if/then)**, and then click **Next**. The **Conditional Data** properties for **Services** page appears.
9. In the **IF** section, click **Add**.
10. Select `Services Name = XService`.
11. Select **Must Exist**.
12. In the **THEN** section, click **Add**.
13. Select `State = Running`.
14. Click **Next**. The **Options** page appears.
15. Select a **Severity** in the drop-down list.
16. Select **Make available for enforcement where possible**.
17. Select **Software Provisioning action**.
18. Select **Install Package** in the drop-down list, and then click **Define Action**. The **Software Provisioning Compliance Remediation** page appears.
19. Select the `XSoftware` package to install if the rule you are configuring fails.
20. Configure the version options to use the selected version, specify a different version, or install the latest version.

21. Select one of the following **Security Options**:

    This option determines if a package is installed or removed based on the state of the signature. Select one of the following options:

    - **Install secure signed package only:** The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.
    - **Skip signature validation when installing a signed package:** (Not Recommended) The package is installed or removed without attempting to verify the signature.
    - **Allow unsigned package to be installed:** (Not recommended) The package is installed or removed even if it is unsigned.

22. Click **OK** to close the page, and then click **Next**. The **Collection filters** page appears.
23. Select the `Services` collection filter.
24. Click **Next**. The **Important** page appears.
25. Review the information, and then click **Finish** to save your rule.

When the Compliance Template is run, if the check for XService running fails, the XSoftware package is installed.

Further Reading

For more information about software provisioning, see VCM online Help, the *VCM Software Provisioning Components Installation and User's Guide*, and the Package Studio online Help.

Getting Started with VCM Management Extensions for Assets 10

Getting Started with VCM Management Extensions for Assets

VCM Management Extensions for Assets (VCMMXA) facilitates the storage of asset data across multi-platform enterprises into a single repository. With VCMMXA, you can integrate and manage data not collected by VCM. This data appears in the VCM Console.

To get started using VCMMXA, follow these steps.

Step 1: Add, Edit, or Delete Hardware and Software Configuration Item Fields.

Step 2: Add Hardware Configuration Items.

Step 3: Add Software Configuration Items.

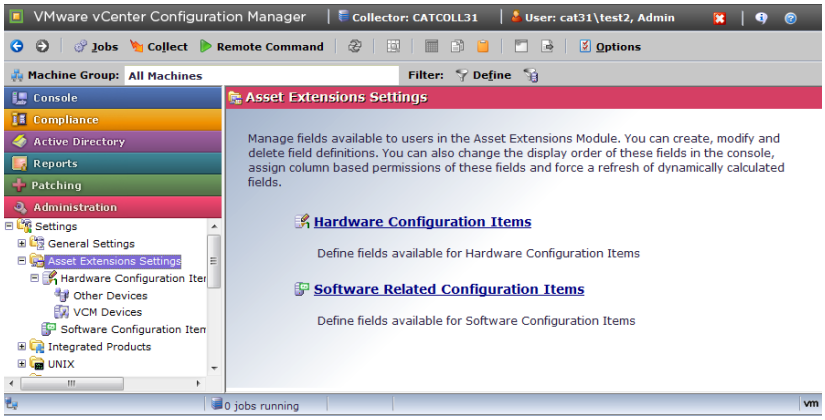
Review Hardware and Software Configuration Item Fields

Before you begin to add asset data to VCM, you should review the default hardware and software fields in VCMMXA and determine if they satisfy the needs of your organization. If not, create, modify, or delete the fields according to your needs.

NOTE VCMMXA Administration functionality is available only to users logged in with the Admin role.

To view the fields, follow these steps.

1. Click **Administration** | **Settings** | **Asset Extensions Settings**. The VCMMXA navigation window appears.



2. Select to configure either the hardware or software configuration item fields.
3. Consider whether the fields are listed in the order in which you want them to appear in the Console. If not, click **Column Order** in the data grid view to reorder the fields to your specifications.
4. By default, dynamic fields are refreshed every six hours. To force a refresh of dynamic fields at any time, click **Refresh Dynamic Fields** in the data grid view.

Modifying Hardware Configuration Item Fields

Use VCMMXA to manage your hardware assets. Add, edit, and delete the hardware configuration items to maintain asset data for the following types of hardware devices:

- **VCM Devices:** Include machines that are currently licensed and managed by VCM. These machines are listed in **Administration** | **Machines Manager** | **Licensed Machines**.
- **Other Devices:** Include machines that are not managed by VCM, as well as other hardware devices, such as bridges, routers, or fax machines.

View Available Fields

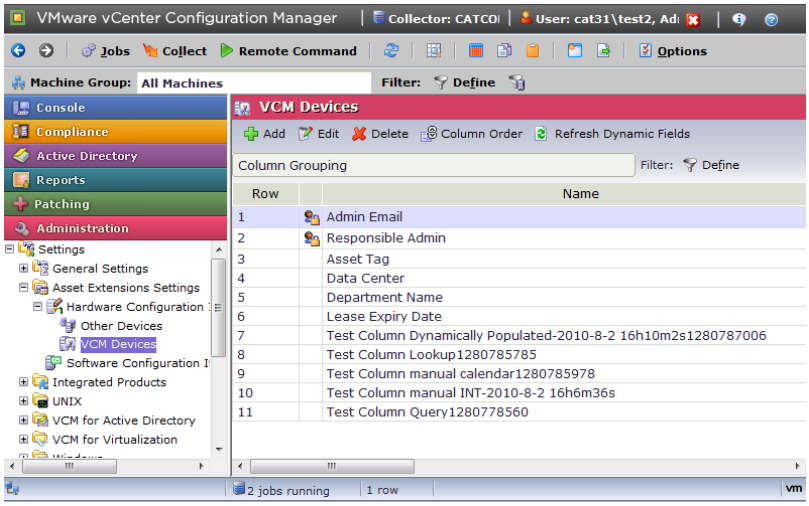
To view the fields available for both VCM Devices and Other Devices, follow these steps.

1. Click **Administration** | **Settings** | **Asset Extensions Settings** | **Hardware Configuration Items** | **VCM Devices or Other Devices**. The data grids in these views contain a list of fields that are available for the type of device you are configuring (VCM Device or Other Device). Each of these fields appears as a column in **Console** | **Asset Extensions** | **Hardware Configuration Items**.
2. Before users populate these fields with asset data, review the fields, and then add, edit, or delete them as desired.

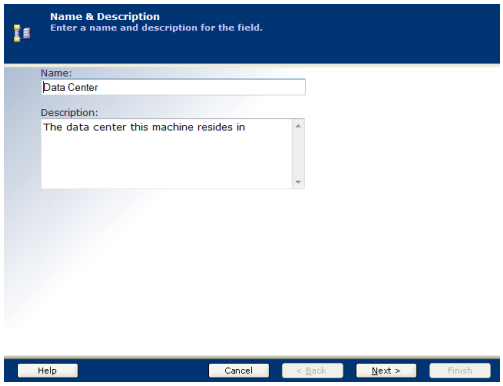
Add or Edit a Hardware Configuration Item Field

To add or edit a hardware configuration item field, follow these steps.

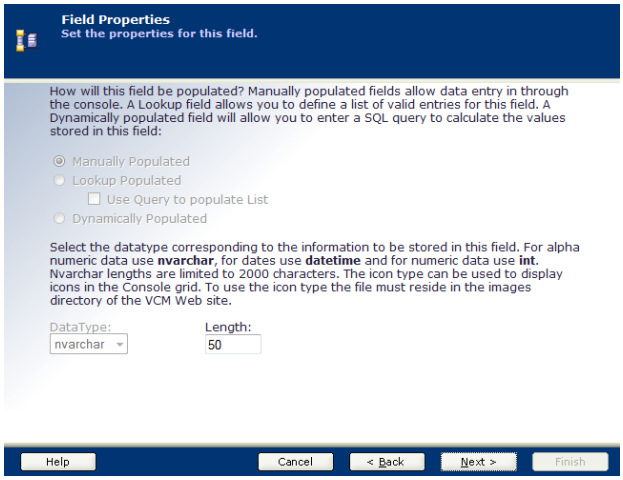
1. Click **Administration** | **Settings** | **Asset Extensions Settings** | **Hardware Configuration Items**. The Hardware Configuration Items view appears.



2. Click **VCM Devices** or **Other Devices**, depending on the type of field you want to delete.
3. If you are editing an existing field, select the field, and then click **Edit**. Otherwise, to add a field, click **Add**. The **Add:Edit Fields** wizard appears.



4. Enter the name and description of the field, and then click **Next**. This name appears as the column heading in **Console** | **Asset Extensions** | **Hardware Configuration Items**.


Field Properties
Set the properties for this field.
How will this field be populated? Manually populated fields allow data entry in through the console. A Lookup field allows you to define a list of valid entries for this field. A Dynamically populated field will allow you to enter a SQL query to calculate the values stored in this field:
Manually Populated
Lookup Populated
Use Query to populate List
Dynamically Populated
Select the datatype corresponding to the information to be stored in this field. For alpha numeric data use nvarchar, for dates use datetime and for numeric data use int. Nvarchar lengths are limited to 2000 characters. The icon type can be used to display icons in the Console grid. To use the icon type the file must reside in the images directory of the VCM Web site.
DataType:
nvarchar
Length:
50
Help
Cancel
< Back
Next >
Finish

5. If you are adding a field, determine how you want this field to be populated. Click the appropriate option button: **Manually** (free-form text), **Lookup** (pick from list of predetermined values), or **Dynamically** (population from another source), and then click **Next**. If you are editing a field, you cannot change the population method. For more information, click **Help**. Otherwise, click **Next**.
6. If you have defined this field as a lookup, the wizard prompts you to define or edit the lookup values. Enter the required information, and then click **Next**.
7. Assign the roles that should have edit access to this field, and then click **Next**. Users with these roles can then edit the values of the field from **Console** | **Asset Extensions** | **Hardware Configuration Items**.
8. Confirm your addition or edit, and then click **Finish**. The field now appears in the **Administration** | **Settings** | **Asset Extension Settings** | **Hardware Configuration Items** | **VCM Devices** or **Other Devices** data grid, and as a column in the **Console** | **Asset Extensions** | **Hardware Configuration Items** | **VCM Devices** data grid.

Delete a Hardware Configuration Item Field

To delete a hardware configuration item field, follow these steps.

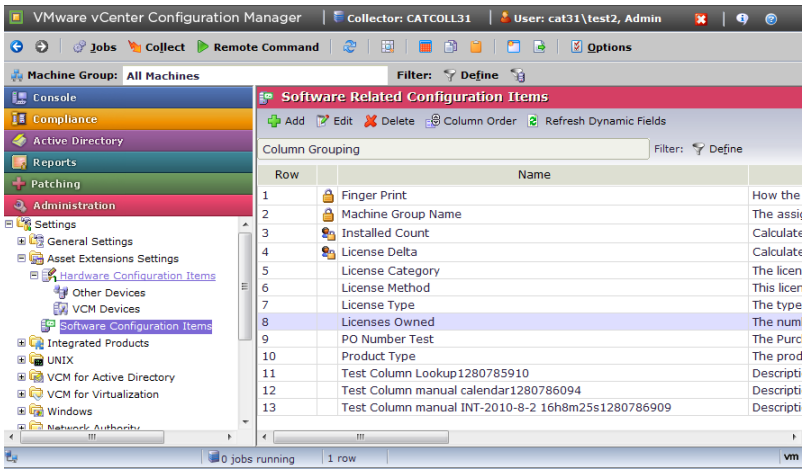
1. Click **Administration** | **Settings** | **Asset Extension Settings** | **Hardware Configuration Items**.
2. Click **VCM Devices** or **Other Devices**, depending on the type of field you want to delete.
3. Select the field, and then click **Delete**. You cannot delete fields marked with a Locked icon.
4. Click **OK** to confirm. VCM deletes the field from VCMMXA.

Modifying Software Configuration Item Fields

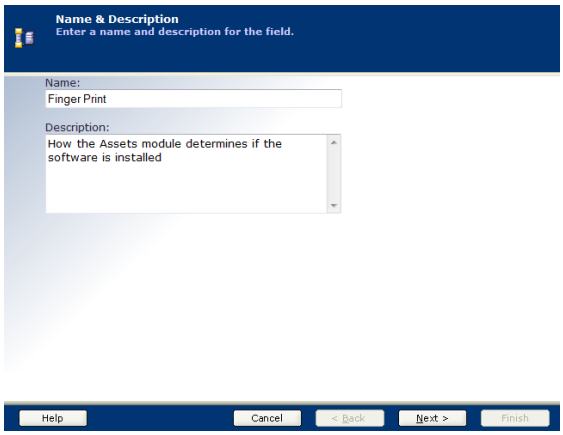
Use VCMMXA to manage your software assets. Add, edit, and delete the software configuration items to maintain asset data for your software.

Add or Edit a Software Configuration Item Field

1. Click **Administration** | **Settings** | **Asset Extension Settings** | **Software Configuration Items**. The Software Related Configuration Items view appears.



2. Review the available fields, and then determine whether you want to add, edit, or delete any of the existing fields. If you are editing an existing field, select the field, and then click **Edit**. Otherwise, to add a field, click **Add**. The **Add:Edit Fields** wizard appears.



3. Enter the name and description of the field. This name appears as the column heading in **Console** | **Asset Extensions** | **Software Configuration Items**. Click **Next**.
4. If you are adding a field, determine how you want this field to be populated. Click the appropriate option button, and then click **Next**. If you are editing a field, you cannot change this information. For more information, click **Help**. Otherwise, click **Next**.
5. If you have defined this field as a lookup, the wizard prompts you to define or edit the lookup values. Enter the required information, and then click **Next**.

6. Assign the roles that should have edit access to this field. Users with these roles can then edit the values of the field from **Console** | **Asset Extensions** | **Software Configuration Items**. Click **Next**.
7. Confirm your addition or edit, and then click **Finish**.The field now appears in the **Administration** | **Settings** | **Asset Extension Settings** | **Software Configuration Items** | **VCMDevices** or **Other Devices** data grid, and as a column in the **Console** | **Asset Extensions** | **Software Configuration Items** data grid.

Delete a Software Configuration Item Field

Use the following procedure to delete a Software Configuration Item field from VCMMXA.

1. Click **Administration** | **Settings** | **Asset Extension Settings** | **Software Configuration Items**.
2. Click **VCM Devices** or **Other Devices**, depending on the type of field you want to delete.
3. Select the field, and then click **Delete**. You cannot delete fields marked with a Locked icon.
4. Click **OK** to confirm. VCM deletes the field from VCMMXA.

Adding Hardware Configuration Items

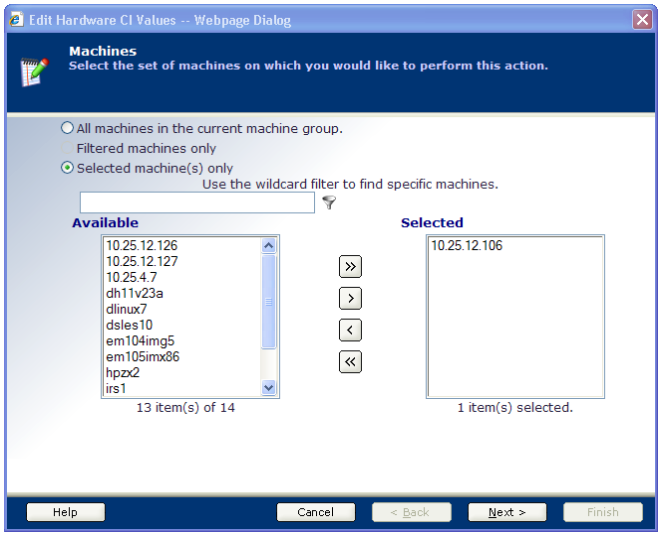
Now that you have configured your VCMMXA fields for both VCM managed and non-managed devices, you can populate those fields with machine-specific data. To begin populating the fields, use the following procedures.

Editing Values for Devices

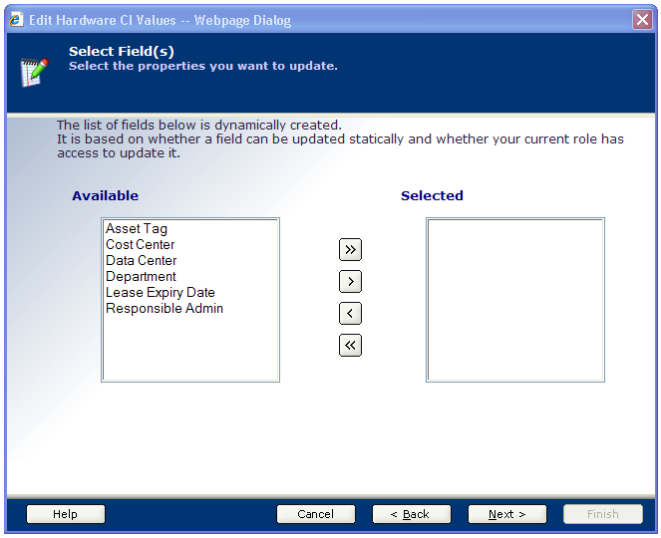
Use the VCM Console to view a list of licensed, VCM-managed machines. Machines appear in this data grid when they are licensed (see Licensing Windows Machines or Licensing UNIX/Linux Machines in the online Help). Machines are removed from this data grid when they are removed from the list of licensed machines in Machines Manager (**Administration** | **Machines Manager** | **Licensed Machines**).

To add information specific to the VCM-managed machines:

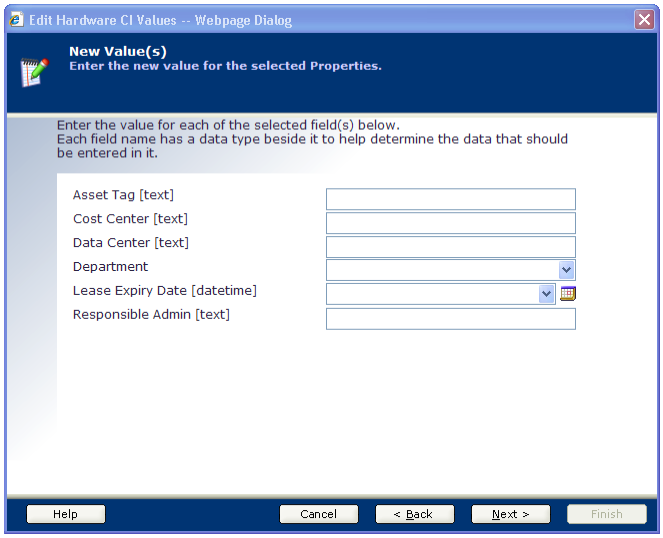
1. Click **Console** | **Asset Extensions** | **Hardware Configuration Items** | **VCM Devices**.
2. Select the machine or group of machines to edit, and then click **Edit Values**. VCM launches the **Edit Hardware CI Values** wizard.



3. Verify the machines you want to edit appear in the **Selected** pane. Click **Next**.



4. Select the fields to edit, and then click **Next**.


Edit Hardware CI Values -- Webpage Dialog
New Value(s)
Enter the new value for the selected Properties.
Enter the value for each of the selected field(s) below.
Each field name has a data type beside it to help determine the data that should be entered in it.
Asset Tag [text]
Cost Center [text]
Data Center [text]
Department
Lease Expiry Date [datetime]
Responsible Admin [text]
Help
Cancel
< Back
Next >
Finish

5. Enter a value for each of the fields displayed, and then click **Next**.
6. Confirm your change, and then click **Finish**. The **VCM Devices** data grid updates the values of the fields for the machines you edited and displays the resulting data.

Modifying Other Devices

In addition to accommodating VCM-licensed machines, VCMMXA also allows you to add up to 135,000 non-VCM managed assets. Use the **Other Devices** node to add, edit, or delete these assets.

To add or edit information specific to other devices, follow these steps.

1. Click **Console** | **Asset Extensions** | **Hardware Configuration Items** | **Other Devices**.
2. If you are adding a device, click **Add**. If you are editing an existing device, select that device, and then click **Edit**.

NOTE If you want to change only the values for that device, and not the device name or description itself, click **Edit Values**, instead of **Edit**. The Edit Values Wizard allows you to quickly edit the specific field values that you select. The **Edit Device** wizard is a longer wizard designed to let you edit the entire device asset record.

3. Follow the prompts through the wizard to complete the action. Click **Help** at any time for more information.

NOTE Use the **Clone** and **Edit Values** functionality to generate a large number of near-identical records. For example, if you are adding more than one record for a specific device type (50 telephones, for example), you can create one record for that device type, and then clone it 50 times. Once you have generated 50 identical records, you can individually select each of the records, then click **Edit Values** to change the fields that distinguish the records from one another (example: Location, or Serial Number). Navigate to **Console | Asset Extensions | Hardware Configuration Items | Other Devices**, and then click **Help** for more information.

To delete a record from the **Other Devices** data grid, follow these steps.

1. Select a record, and then click **Delete**.
2. Click **OK** to confirm your deletion. VCMMXA deletes the requested record from the Other Devices data grid.

Adding Software Configuration Items

Use the **Software Configuration Items** node to build a list of software assets. You can add values to the inventory and manage other aspects of software, such as license counts, license expiration dates, or even custom fields that support your organization's processes.

When you configure the values for these fields, they are available in Compliance also, where you can create rules to actively check inventory. For example, use options in VCM Compliance to verify that your install count for licensed software is below your overall purchase license count. For more information about VCMMXA-specific issues in Compliance, click **Console | Asset Extensions**, and then click **Help**.

To add or edit Software Configuration Items, follow these steps.

1. Click **Console | Asset Extensions | Software Configuration Items**.
2. If you are adding software, click **Add**. If you are editing an existing software asset record, select that row, and then click **Edit**.
3. If you want to change the values for that software entry, and not the software asset name or description itself, click **Edit Values**, instead of **Edit**. The **Edit Values** wizard allows you to select the field values you want to edit, and then change them. The **Edit** wizard is designed to let you edit the entire software asset record.

NOTE Use the **Clone** and **Edit Values** functionality to generate a large number of near-identical records. For example, if you are adding more than one record for a specific software item, you can create one record for that item, and then clone it 50 times. Once you have generated 50 identical records, you can individually select each of the records, then click **Edit Values** to change the fields that distinguish the records from one another. Navigate to **Console | Asset Extensions | Software Configuration Items**, and then click **Help** for more information.

To delete a record from the Software Configuration Items data grid, follow these steps.

1. Select the record, and then click **Delete**.
2. Click **OK** to confirm your deletion. VCMMXA deletes the requested record from the **Software Configuration Items** data grid.

Further Reading

For information on how to customize for your environment, refer to Customizing VCM. Each of these areas regarding customization also applies to VCMMXA. You can also read Maintaining VCM after Installation for important information regarding additional data retention settings and database maintenance steps that you should take.

When using VCMMXA, refer to the online Help for specific information.

Getting Started with VCM Service Desk Integration 11

Getting Started with Service Desk Integration

VCM Service Desk Integration allows you to track planned and unplanned changes to managed machines in your organization, and to integrate these changes with your organization's change management process.

When Service Desk Integration is licensed, integrated with VCM Service Desk Connector, and activated, it temporarily halts any requested change to a VCM-managed machine while VCM integrates with the Service Desk application to pass the change through a predefined change management process or workflow. Once the change is approved through the workflow, VCM reinstates the change requested on the Agent machine(s), based upon machine criticality.

VCM Service Desk Connector communicates with both VCM and your Service Desk application to help users track and manage all VCM-initiated planned and unplanned changes across an organization. Any change to a VCM-managed machine that is requested in VCM must advance through the defined workflow before being executed. The workflow definition varies by customer and is dependent upon the configuration implemented during the VMware services engagement and as determined by the customer's change management process.

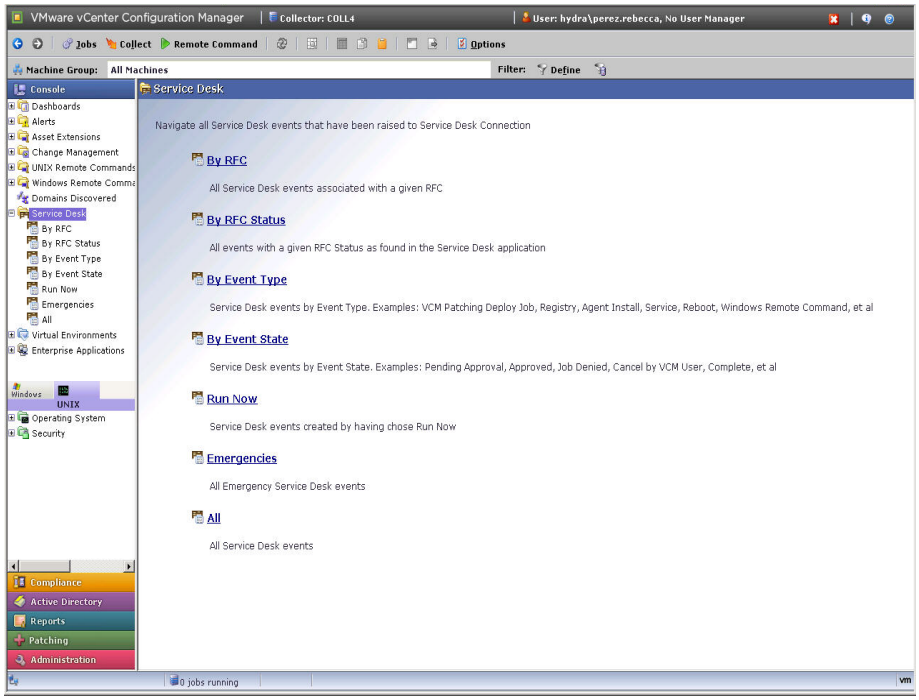
If you have licensed VCM Service Desk Integration, will you be able to see the Service Desk nodes. However, you must arrange a services engagement to "turn on" Service Desk functionality, and configure and implement this component. Contact VMware Customer Support to determine the requirements for your integration. Once VMware Customer Support has enabled VCM Service Desk Integration, they will give you an overview of how to use the product in your organization. You may also refer to the online Help for more information on how to use VCM Service Desk Integration.

Service Desk Integration in the Console

The Service Desk node provides a single entry point for viewing all VCM-related Service Desk events. Click any sub-node beneath the Service Desk node to view data by that variable. For example, click **By RFC** to view the data for a single Request For Change (RFC). In the By RFC sub-node, select any of the listed RFCs to view the data for that item only.

The data views shown below are the default VCM Service Desk Integration views. Your configuration may differ, based on your organizational requirements and specific implementation.

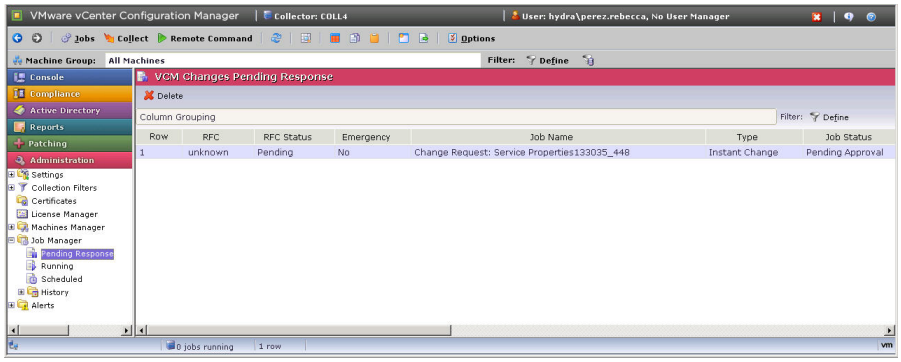
Click **Console** | **Service Desk** to display the VCM Service Desk Integration node.


VMware vCenter Configuration Manager
Collector: COLL4
User: hydra\perez.rebecca, No User Manager
Jobs
Collect
Remote Command
Options
Machine Group:
All Machines
Filter:
Define
Console
Service Desk
Navigate all Service Desk events that have been raised to Service Desk Connection
By RFC
All Service Desk events associated with a given RFC
By RFC Status
All events with a given RFC Status as found in the Service Desk application
By Event Type
Service Desk events by Event Type. Examples: VCM Patching Deploy Job, Registry, Agent Install, Service, Reboot, Windows Remote Command, et al
By Event State
Service Desk events by Event State. Examples: Pending Approval, Approved, Job Denied, Cancel by VCM User, Complete, et al
Run Now
Service Desk events created by having chose Run Now
Emergencies
All Emergency Service Desk events
All
All Service Desk events
Compliance
Active Directory
Reports
Patching
Administration
0 jobs running

Service Desk Integration in Job Manager

When VCM Service Desk Integration is licensed and activated, it suspends any requested change to a VCM-managed machine while VCM integrates with the Service Desk application to pass the change through a change management process. If a job was suspended in VCM, it appears in **Administration** | **Job Manager** | **Pending Response**. Once the job is approved, it is released to run, thereby appearing in either the **Job Manager** | **Running** or **Job Manager** | **Scheduled nodes**. Jobs integrated with VCM Service Desk Integration are listed by RFC in the Job Manager data grids.

Click **Administration** | **Job Manager** to display the VCM Job Manager node.



NOTE Jobs for VCM Patching-managed machines appear in the Patching Job Manager, not the VCM Job Manager. Locate these jobs at: **Patching** | **Administration** | **Job Manager**. Click **VCM Patching Administration** | **Job Manager** | **Pending Response** to locate jobs that are currently awaiting approval. Click **VCM Patching Administration** | **Job Manager** | **Running or VCM Patching Administration** | **Job Manager** | **Scheduled** to locate approved jobs that are currently running, or are scheduled to run.

Further Reading

Refer to Customizing VCM for information on how to customize for your environment. Each of these areas regarding customization also applies to VCM for Service Desk Integration. You can also read Maintaining VCM after Installation for important information regarding additional data retention settings and database maintenance steps which should be taken.

When using VCM for Service Desk Integration, refer to the Help for specific task information. To access the Help, click the **Help** button, located on the Portal toolbar.

Getting Started with VCM for Active Directory 12

VCM for Active Directory (AD) collects AD objects across Domains and Forests, and displays them through a single console. This data is consolidated and displayed under the Active Directory slider, providing a logical grouping of AD object and configuration information, allowing you to view your AD structure, troubleshoot issues, and detect change.

Data can be filtered, sorted, and grouped to allow you to pinpoint the specific area in which you are interested. You can also view a subset of your AD (a Forest, Domain, or specific OU branch) by setting the AD Location in the global zone at the top of the VCM Portal. Dashboards display high-level roll up information in graphical form, Alerts can be configured to notify you when there is a problem or misconfiguration, and Change Management tracks changes to the AD objects or configuration by data class.

Before you begin collecting Active Directory data with VCM for Active Directory, you must complete the following required steps. These steps are explained in this chapter.

1. Making VCM aware of your Domain Controllers
2. Configuring VCM for Active Directory as an additional product
3. Performing an Active Directory data collection
4. Exploring Active Directory collection results

Making VCM Aware of Domain Controllers

The first step in using VCM for Active Directory (AD) is to make VCM aware of the Domain Controllers (DCs), and license them as Windows servers. Once they are licensed, you can then perform an initial machines collection to make them available to VCM for Active Directory (AD).

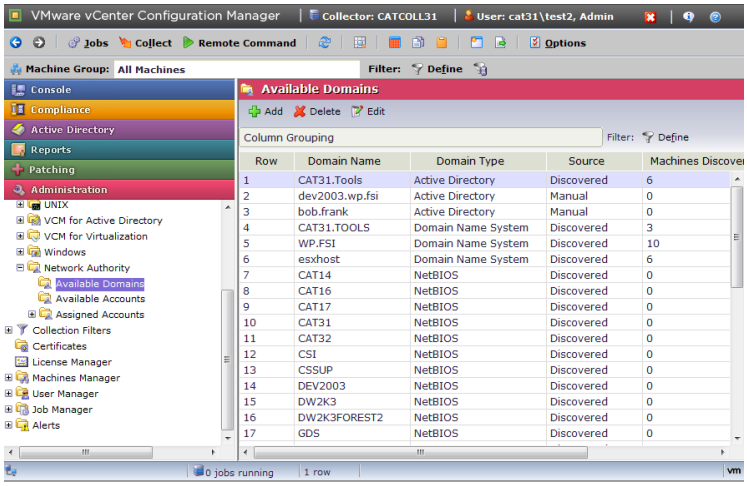
Follow the steps listed below to make VCM aware of your DCs and to perform an initial collection:

1. Confirming the Presence of Domains
2. Adding and Assigning Network Authority Accounts
3. Discovering Domain Controllers
4. Verifying Domain Controller Machines in Available Machines
5. Licensing and Deploy the Agent
6. Performing a Machine Data Type Collection

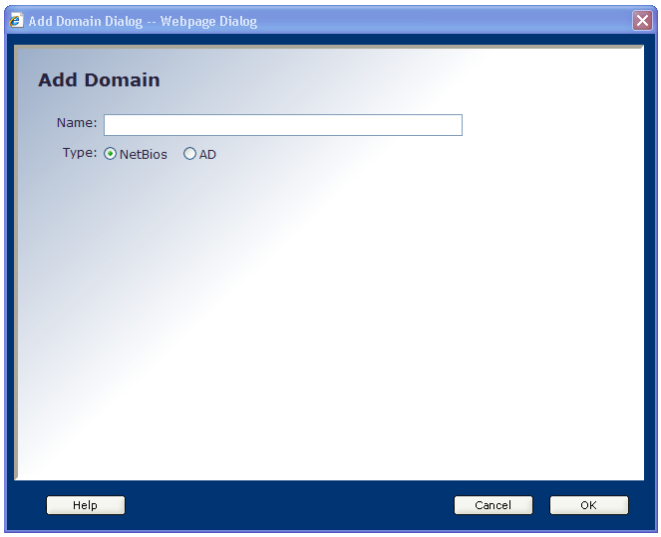
Confirming the Presence of Domains

Prior to setting up VCM for Active Directory, you must confirm that all fully-qualified DNS Domains that you want to manage have been discovered by VCM. Domains are discovered during the VCM installation process; however, you may need to manually add Domains that were unavailable during the installation process.

1. Click **Administration** | **Settings** | **Network Authority** | **Available Domains**.



2. Confirm that all Domains that you want to manage with VCM for Active Directory are displayed in the data grid with their fully-qualified DNS names and a **Domain Type** of Active Directory.
3. If an Active Directory Domain is not listed in the data grid, click **Add**. The **Add Domain** dialog box appears.



4. In the **Name** text box, type a fully-qualified DNS Domain name,
5. Select the **AD** type.
6. Click **OK**. Repeat the adding process to add additional Active Directory Domains.

Adding and Assigning Network Authority Accounts

Before you can perform any type of action (Discovery, Collection, and so forth), the Collector must gain access to each Domain to interact with the selected Domain Controllers (DCs) in the organization.

A VCM network authority account must have administrator rights and be added for each Domain to be managed in the organization. Once these accounts have been added, they must be assigned to Domains.

If you want to:

- Add a new Network Authority Account, refer to "Checking the Network Authority" on page 54. Perform these steps for each Domain in which you will manage machines.
- Assign the Network Authority Account to each Domain, refer to "Assigning Network Authority Accounts" on page 55. Perform these steps for each Domain that you plan to perform collections against.

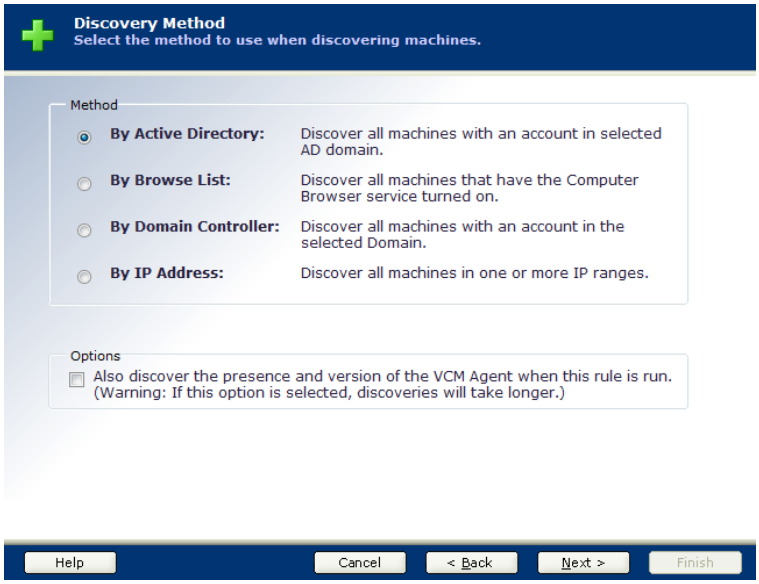
IMPORTANT When assigning accounts, assign an available account to both the NetBIOS and Active Directory Domains.

Discovering Domain Controllers

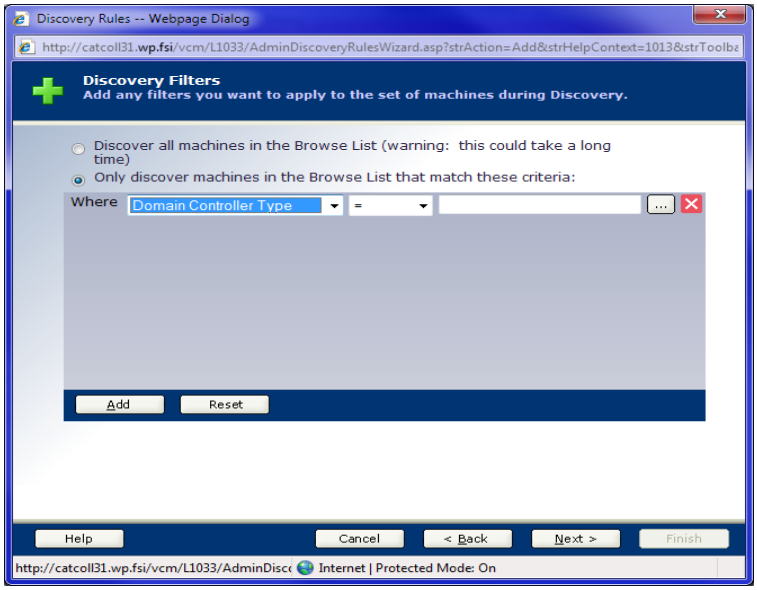
VCM offers several options for the discovery of Domain Controllers in an organization. If you know which Domain Controllers are in your organization, then you can manually add them to the list of Available Machines. To manually add a machine, click **Administration | Machines Manager | Available (Windows) Machines**, and then click **Add Machines**.

If you have a large number of Domain Controllers to be manually added to VCM, and you only want Domain Controllers to appear in the Available Machines list, we recommends that you perform the following Browse List discovery using Domain Controller Type as a filter.

1. Click **Administration | Machines Manager | Discovery Rules**.
2. Click **Add**. The **Discovery Rules** page appears.
3. Type a **Name** and **Description** for this new discovery rule, then click **Next**. The **Discovery Method** page appears.


Discovery Method
Select the method to use when discovering machines.
Method
By Active Directory:
Discover all machines with an account in selected AD domain.
By Browse List:
Discover all machines that have the Computer Browser service turned on.
By Domain Controller:
Discover all machines with an account in the selected Domain.
By IP Address:
Discover all machines in one or more IP ranges.
Options
Also discover the presence and version of the VCM Agent when this rule is run. (Warning: If this option is selected, discoveries will take longer.)
Help
Cancel
< Back
Next >
Finish

4. Select **By Browse List**, then click **Next**. The **Discovery Filters** page appears.


Discovery Rules -- Webpage Dialog
Discovery Filters
Add any filters you want to apply to the set of machines during Discovery.
Discover all machines in the Browse List (warning: this could take a long time)
Only discover machines in the Browse List that match these criteria:
Where
Domain Controller Type
=
Add
Reset
Help
Cancel
< Back
Next >
Finish
Internet | Protected Mode: On

5. Select **Only discover machines in the Browse List that match these criteria**.
6. Specify the filter parameters. Select `Domain Controller Type <> "` (two single quotes).
7. Click **Next**. The **Important** page appears.
8. For the **Would you like to run this Discovery Rule now**? option, select **Yes**.
9. Click **Finish**.

IMPORTANT Click **Administration | Job Manager | History | Instant Collections | Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Verifying Domain Controller Machines in Available Machines

Once your Domain Controller discovery is completed, verify that your Domain Controllers are available for licensing and Agent installation.

1. Click **Administration | Machines Manager | Available Machines | Available Windows Machines**.
2. Verify that the domain controller machines are available in the Domains that you added in your discovery rule.

Licensing and Deploying the VCM Agent

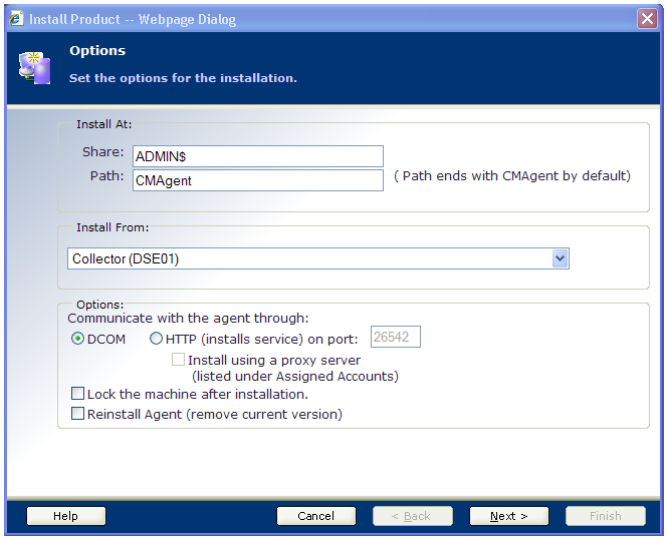
All discovered Domain Controller machines appear in the **Available Windows Machines** list. You can group them by type (workstations or machines) and pick each Domain Controller individually or license and deploy the Agent to multiple Domain Controllers at the same time.

IMPORTANT If you are licensing and deploying the Agent on a Windows 2008 or Vista machine, you must first disable the User Account Control (UAC) on the target machine. See Disabling UAC for Agent Installation for more information.

NOTE Your license count determines how many machines (specifically Domain Controllers in VCM for Active Directory) that you can license. You should begin licensing Domain Controllers that have a Status Connection State of **OK**. If a connection state other than **OK** exists, you may need to work with Customer Support to assist you with troubleshooting the connection to that Domain Controller.

---

1. Click **Administration | Machines Manager | Available Machines | Available Windows Machines**.
2. In the data grid, select the Domain Controllers you are licensing. To select multiple Domain Controllers, use Shift-click or Ctrl-click.
3. Click **License**. The **Machines** page of the **Available Machines License** wizard appears.
4. By default, the machines selected in the data grid are displayed in the **Selected** list. To license additional Domain Controllers, double-click the machine name in the Available list to move it to the Selected list.
5. Select the **Install VCM agents for the selected machines** check box.
6. Click **Next**. The **Product License Details** page appears.
7. View your product license details, and then click **Next**. The **Important** page appears, reminding you that you are installing the Agent.
8. Click **Next**. The **Options** page appears.



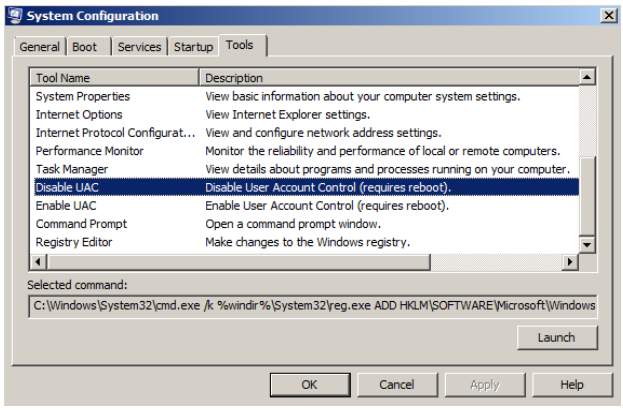
9. Verify the method used for communication. The default communication method is DCOM. For most VCM for Active Directory configurations, the default values in this screen should be used.
   Click **Next**. The **Schedule** page appears.
10. Select **Run Action now**, and then click **Next**.
11. Click **Finish**. The Selected Domain Controllers are moved from the **Available Machines** list to the **Licensed Machines** list, and an Install job is submitted to initiate the Agent installation on each Domain Controller.

Disabling UAC for Agent Installation

The following steps are required only if you are installing the Agent on a Windows 2008 or Vista machine. When installing the Agent on Windows 2008 or Vista, you must disable the User Account Control (UAC), install the Agent, and then re-enable the UAC.

Disabling UAC on One Machine

1. On the target Windows 2008 machine, click **Start** | **Run**. The **Run** dialog box appears.
2. Type **msconfig** in the **Open** text box.
3. Click **OK**. The **System Configuration** dialog box appears. (This dialog box differs for Windows 2008 R2 machines.)



4. Click the **Tools** tab.
5. In the **Tool Name** list, select **Disable UAC**.
6. Click **Launch**. A **Command** window displays the running action. When the command is completed, close the window.
7. Close the **System Configuration** dialog box.
8. Restart the machine to apply the changes.
9. Install the Agent as specified in Licensing and Deploying the VCM Agent.
10. After installing the Agent on the target machine, re-enable UAC. To enable, perform the steps specified above. In Step 5, select **Enable UAC** in the **Tool Name** list.
11. Restart the machine to apply the changes.

Disabling UAC using Group Policy

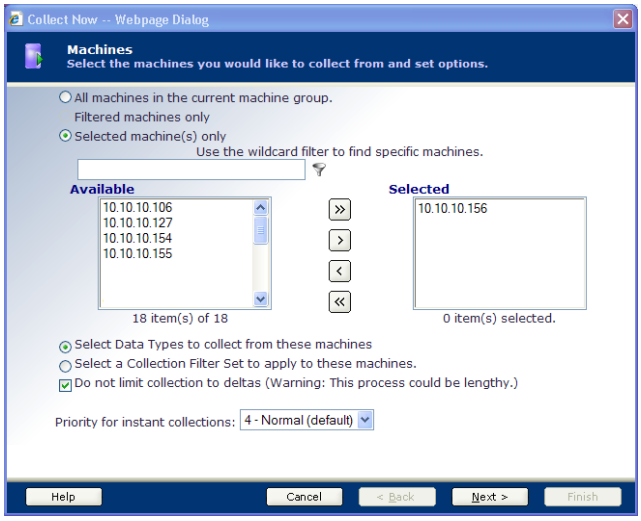
Use the following procedure to disable the UAC on multiple machines. The instructions assume you have configured the Windows 2008 and Vista machines targeted for Agent install in a common Active Directory domain/OU.

1. On a Domain Controller, click **Start | Run**. The **Run** dialog box appears.
2. Type **mmc** in the **Open** text box.
3. Click **OK**. The **Console** window appears.
4. Select **Console Root**, and then click **File | Add/Remove Snap-in. The Add or Remove Snap-ins** dialog box appears.
5. In the **Available snap-ins** list, double-click **Group Policy Management Editor**. The **Select Group Policy Object** dialog box appears.
6. Click **Browse**. The **Browse for a Group Policy Object** dialog box appears.
7. On the **Domains/OUs** tab, select the domain/OU to which the target machines belong, and then click **OK**.
8. On the **Select Group Policy Object** dialog box, click **Finish**.
9. On the **Add or Remove Snap-Ins** dialog box, click **OK**.
10. The domain/OU policy is added to the Console Root in the left pane.
11. Expand the added domain/OU and browse to **Computer Configuration | Policies | Windows Settings| Security Settings | Local Policies | Security Options**.
12. In the right pane, locate the **User Access Control** policies. On each of the policies specified below, right-click and select **Properties**. Configure as follows:
    - **User Account Control: Behavior of the elevation prompt for administration in Admin Approval Mode:** Elevate without prompting.
    - **User Account Control: Detect application installations and prompt for elevation:** Disabled
    - **User Account Control: Run all administrators in Admin Approval Mode:** Disabled
13. Restart the machine to apply the changes.
14. Install the Agent as specified in the previous section, "Licensing and Deploying the VCM Agent".
15. After installing the Agent on the target machines, re-enable UAC. To enable, perform the steps specified above. In Step 5, change the policies to Enabled.
16. Restart the machine to apply the changes.

Performing a Machine Data Type Collection

Now you must perform a collection based on the **Machines Data** type. Refer to Performing an Initial Collection for detailed procedures on how to perform a collection.

1. Configure the **Machines** page (Step 2) as follows:



   - Add only your Domain Controllers to the **Selected** list.
   - Select the **Do not limit collection to deltas** check box. Selecting this option ensures that a full collection will occur during set up of VCM for Active Directory.

2. On the **Data Types** page (Step 3), select **Machines** .

IMPORTANT Click **Administration** | **Job Manager** | **History** | **Instant Collections** | **Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Configuring VCM for Active Directory as an Additional Product

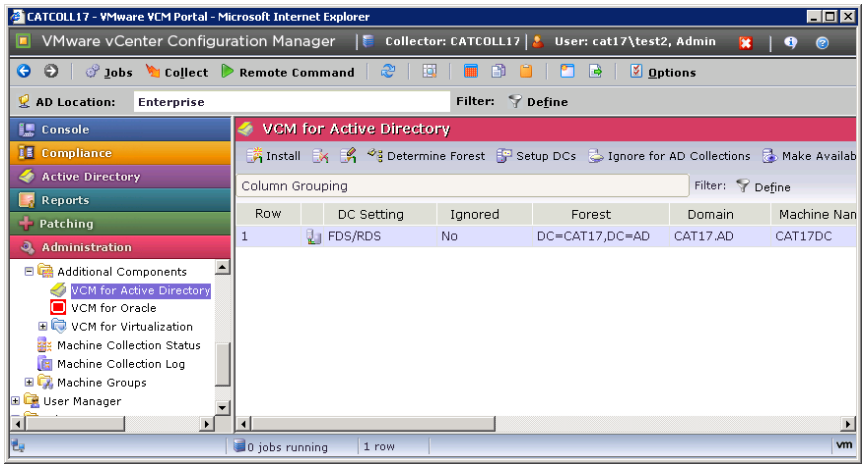
Now that VCM is aware of your Domain Controllers, follow the steps listed below to configure VCM for AD as an additional product.

1. Deploy VCM for AD to the Domain Controllers
2. Run the Determine Forest Action
3. Run the Setup DCs Action

Deploying VCM for AD to the Domain Controllers

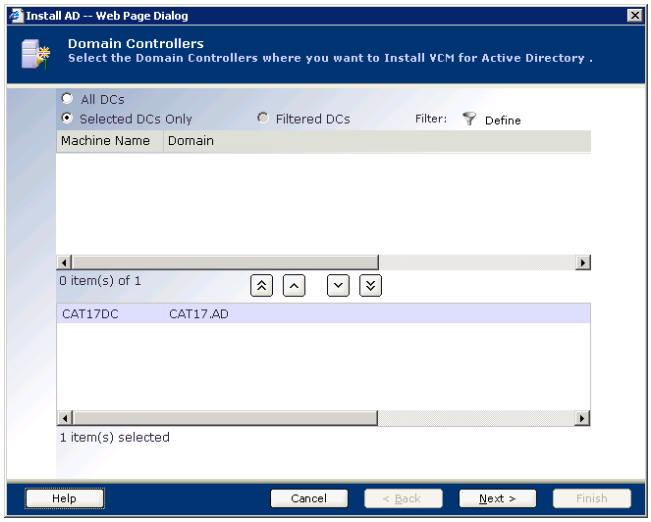
Use the following procedure to install VCM for Active Directory on each Domain Controller from which you want to collect data.

1. Click **Administration** | **Machines Manager** | **Additional Components** | **VCM for Active Directory**.



NOTE If the Domain Controllers that you want to collect from are not listed in **Additional Products** | **VCM for Active Directory** node, you may need to confirm or repeat the procedures described in the previous sections.

2. Click **Install** to deploy VCM for Active Directory to the Domain Controllers from which you want to collect Active Directory data.
3. Select the Domain Controllers on which you want to install VCM for Active Directory. We recommend that you install VCM for Active Directory on all Domain Controllers.



NOTE VCM for AD will operate with only a single domain controller configured with VCM for AD as both the FDS/RDS (Forest Data Source/Replication Data Source). However, to collect important non-replicated attributes such as Last Logon, it is essential that you configure as many domain controllers

as possible with VCM for AD.

If you have machines that you plan to promote to Active Directory machines, but have not yet done so, you must install VCM for Active Directory manually. Go to **Program Files\VMware\VCM\AgentFiles** and run the `ADProductInstall.exe` installer.

4. Click **Next**.
5. Verify that **Run Action now** is selected, then click **Finish**.

IMPORTANT Click **Administration | Job Manager | History | Other Jobs | Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Running the Determine Forest Action

VCM for Active Directory requires a Forest determination for all Domain Controllers so that it can proceed with schema and structure collection. Therefore, your next step is to perform a Forest Determination for all of the licensed Domain Controllers in your list.

1. Click **Administration | Machines Manager | Additional Components | VCM for Active Directory**.
2. Click **Determine Forest**. The **Domain Controllers** page appears.
3. Move all Domain Controllers for which you want to determine the Forest to the lower pane. The Forest determination job will run only on those DCs where VCM for Active Directory is installed. We recommend determining the Forest for all Domain Controllers in the list.
4. Click **Next**. The **Important** page appears.
5. Click **Finish**.
6. Upon completing the Setup DCs action, a collection will be submitted to the selected DCs. Forest information will be displayed in the **Administration | Machines Manager | Additional Products | VCM for Active Directory** data grid. Each Setup DCs job initiates the following three jobs:
   - AD Schema Collection
   - AD Specifier Collection
   - AD Structure Collection

IMPORTANT Click **Administration | Job Manager | History | Instant Collections | Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Running the Setup DCs Action

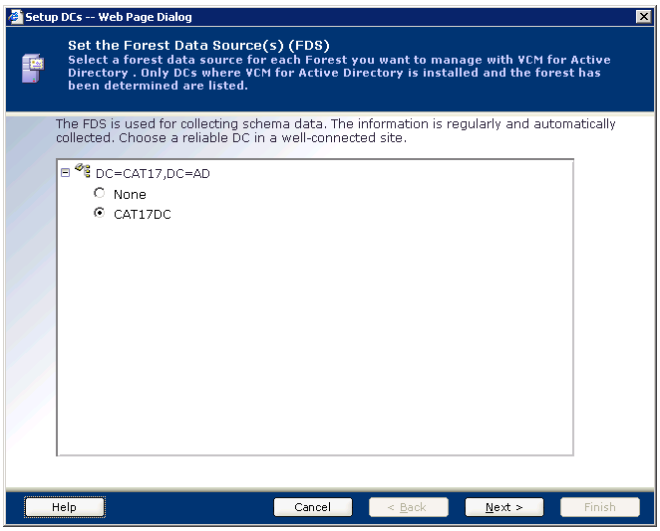
The final step that you must take prior to collecting AD objects from your Domain Controllers is to run the Setup DCs action. VCM for Active Directory collects the AD schema and your AD structure during the Setup DCs action. A Forest Data Source (FDS) and Replication Data Source (RDS) must be specified before Active Directory data is collected from a Forest.

VCM for Active Directory uses the FDS as a resource for all required Forest-level information. One Domain Controller for each Forest must be distinguished as the FDS in order for VCM for Active Directory to perform collections. The RDS serves as the Domain Controller from which all replicated data will be collected. VCM for Active Directory requires one RDS per Domain so that collections on replicated attributes are only performed on a single DC. All other Domain Controllers which have VCMfor Active Directory installed will only be accessed during collections for non-replicated attributes.

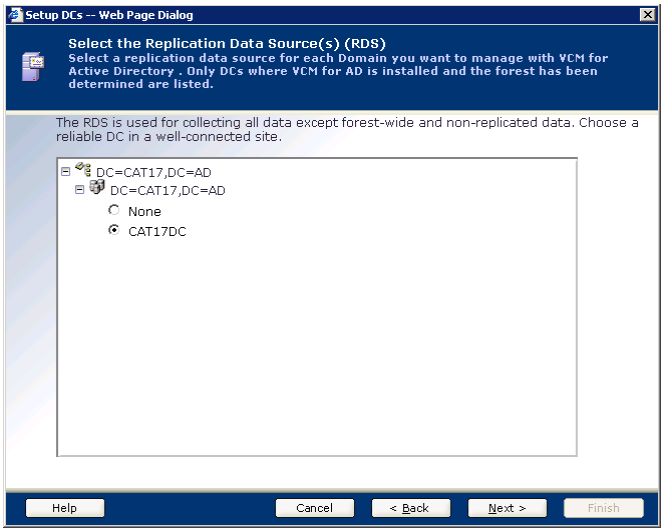
NOTE A single Domain Controller may be selected as both an FDS and RDS. We recommend selecing DCs with reliable connections and availability to serve in the FDS and RDS capacities for VCM for Active Directory collections.

If you change your RDS, any data previously collected from the RDS is not purged. The data is refreshed when you run a new collection and gather data from the new RDS.

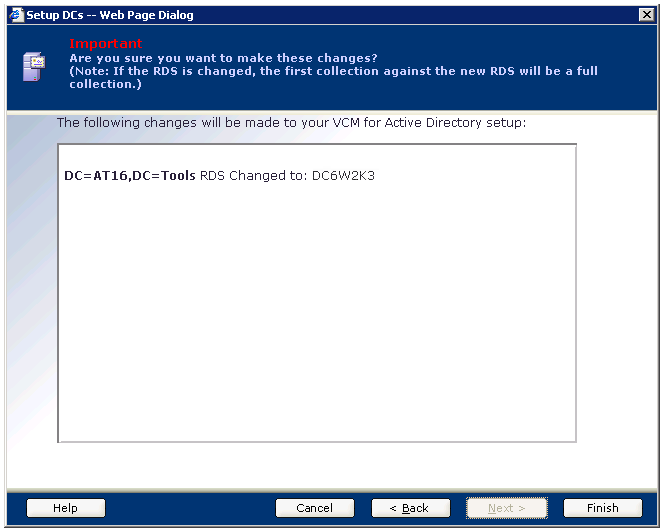
1. Click **Administration | Machines Manager | Additional Components | VCM for Active Directory**.
2. Click **Setup DCs**. The **Set the Forest Data Source(s) (FDS)** page appears.


Setup DCs -- Web Page Dialog
Set the Forest Data Source(s) (FDS)
Select a forest data source for each Forest you want to manage with VCM for Active Directory . Only DCs where VCM for Active Directory is installed and the forest has been determined are listed.
The FDS is used for collecting schema data. The information is regularly and automatically collected. Choose a reliable DC in a well-connected site.
DC=CAT17,DC=AD
None
CAT17DC
Help
Cancel
< Back
Next >
Finish

3. Select a Forest Data Source (FDS) for each Forest to be managed in VCM for Active Directory, and then click **Next**. The **Select the Replication Data Source(s) (RDS)** page appears.


Setup DCs -- Web Page Dialog
Select the Replication Data Source(s) (RDS)
Select a replication data source for each Domain you want to manage with VCM for Active Directory . Only DCs where VCM for AD is installed and the forest has been determined are listed.
The RDS is used for collecting all data except forest-wide and non-replicated data. Choose a reliable DC in a well-connected site.
DC=CAT17,DC=AD
DC=CAT17,DC=AD
None
CAT17DC
Help
Cancel
< Back
Next >
Finish

4. Select a Replication Data Source (RDS) for each Domain that you want to be managed by VCM for Active Directory. Click Next. The **Important** page appears.


Setup DCs -- Web Page Dialog
Important
Are you sure you want to make these changes?
(Note: If the RDS is changed, the first collection against the new RDS will be a full collection.)
The following changes will be made to your VCM for Active Directory setup:
DC=AT16,DC=Tools RDS Changed to: DC6W2K3
Help
Cancel
< Back
Next >
Finish

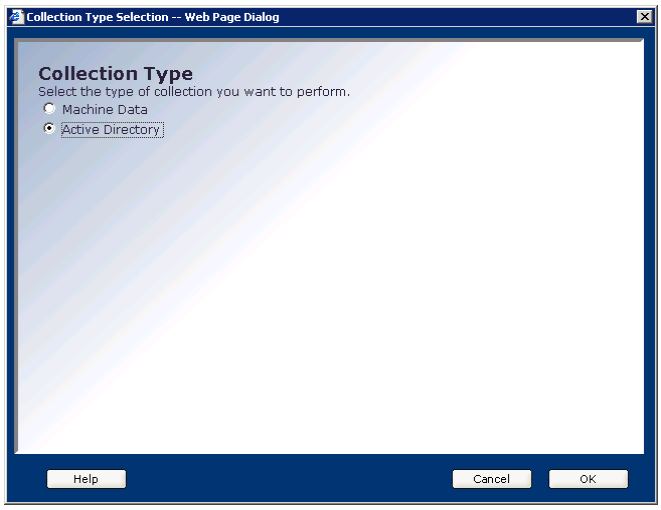
5. Click **Finish**.
6. When the Setup DCs action is completed, VCM for Active Directory performs a schema and a structure collection. The information obtained from the structure collection identifies the OU structure which supports the use of VCM for Active Directory.

IMPORTANT Click **Administration** | **Job Manager** | **History** | **Instant Collections** | **Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

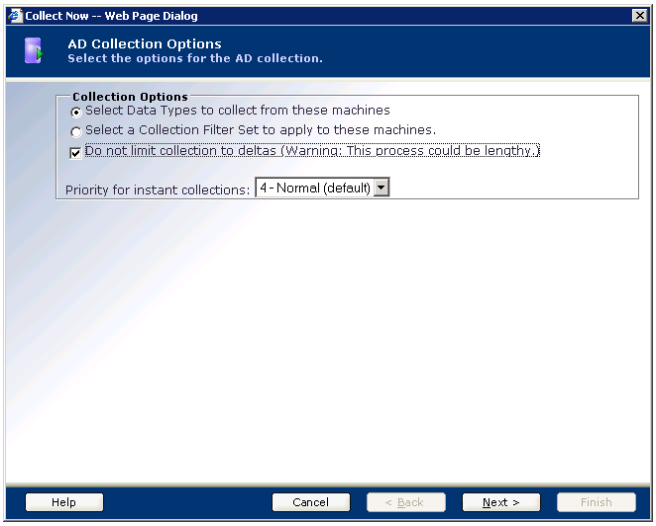
Performing an Active Directory Data Collection

You are now ready to perform your first collection of Active Directory objects using the same collection wizard used for Windows and UNIX/Linux collections. The first time you run an AD collection, the Agent will return all the objects and attributes from your Active Directory specified in the default filter set.

1. Click **Collect**, located on the Portal toolbar. The **Collection Type Selection** dialog box appears.



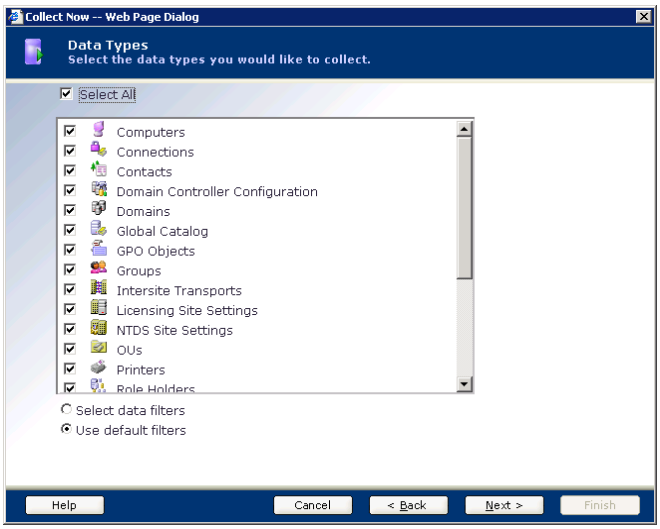
2. For the **Collection Type**, select **Active Directory**.
3. Click **OK**. The **Collect Now** wizard appears, displaying the **AD Collection Options** page.


Collect Now -- Web Page Dialog
AD Collection Options
Select the options for the AD collection.
Collection Options
Select Data Types to collect from these machines
Select a Collection Filter Set to apply to these machines.
Do not limit collection to deltas (Warning: This process could be lengthy.)
Priority for instant collections:
4 - Normal (default)
Help
Cancel
< Back
Next >
Finish

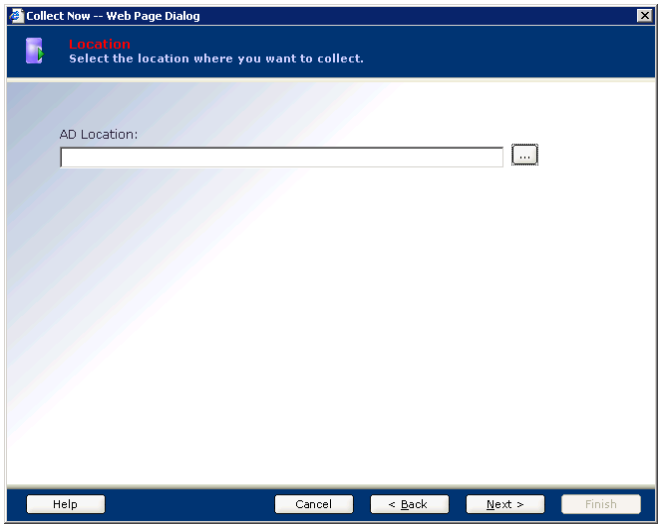
4. Click **Select Data Types to collect from these machines**.
5. To ensure that a full collection will occur during setup of VCM for Active Directory, click the **Do not limit collection to deltas** check box.

   NOTE The delta collection feature makes subsequent collections run faster and more efficiently than the initial collection. For the initial collection, make sure that you click the check box so that the delta feature is disabled.

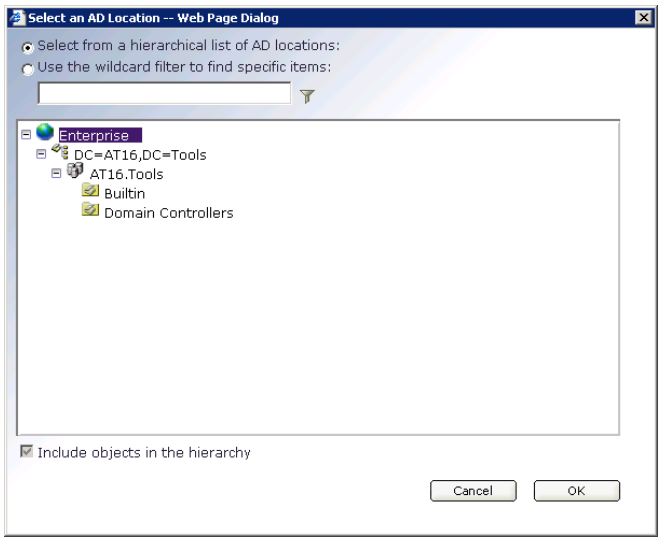
6. Click **Next**.The **Data Types** page appears.



7. Click **Select All**.
8. Select the **Use default filters** is selected option.
9. Click **Next**. The **Location** page appears.



10. To specify a location click the lookup ellipsis button (...). The **Select an AD Location** page appears.



11. Expand the **Enterprise** tree, and then select an AD Location.
12. Click **OK**, to close the page.
13. On the **Location** page, click **Next**.
14. Click **Finish**.

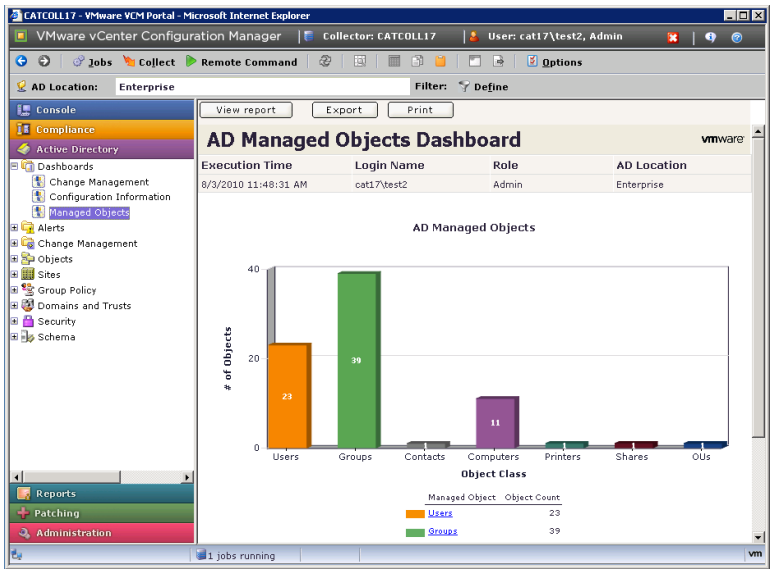
IMPORTANT Click **Administration** | **Job Manager** | **History** | **Instant Collections** | **Past 24 Hours** to verify that all jobs have completed before proceeding to the next step.

Exploring Active Directory Collection Results

Now that you have performed an initial Active Directory collection, you can explore that data within the Portal. VCM for AD presents enterprise-wide, summary information in graphical SSRS charts that you can view, export, or print. Each VCM for AD Dashboard is run only when the node is selected against the current data available in the CMDB. Therefore, Dashboard data is only current as of the time was collected. In addition, it may take time for the data to display based upon the volume or complexity of the data requested.

Active Directory Dashboards

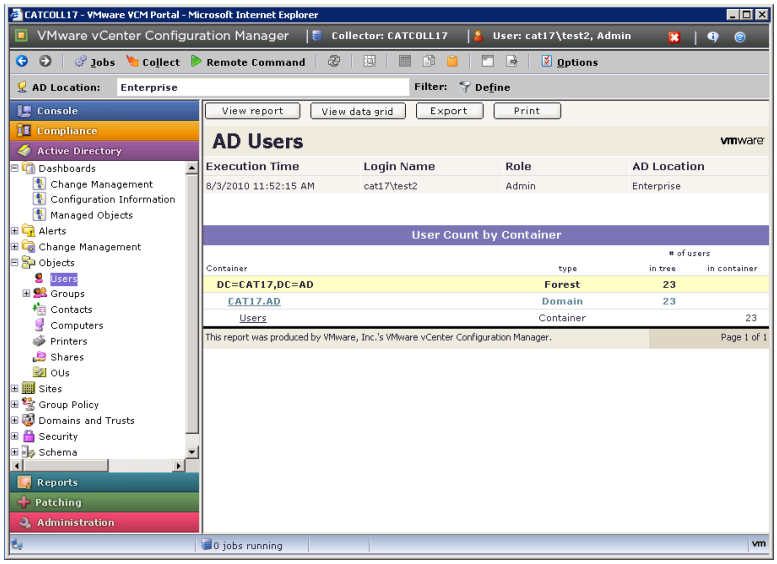
Begin by looking at the VCM for Active Directory dashboard under **Active Directory** | **Dashboards** | **Managed Objects**.



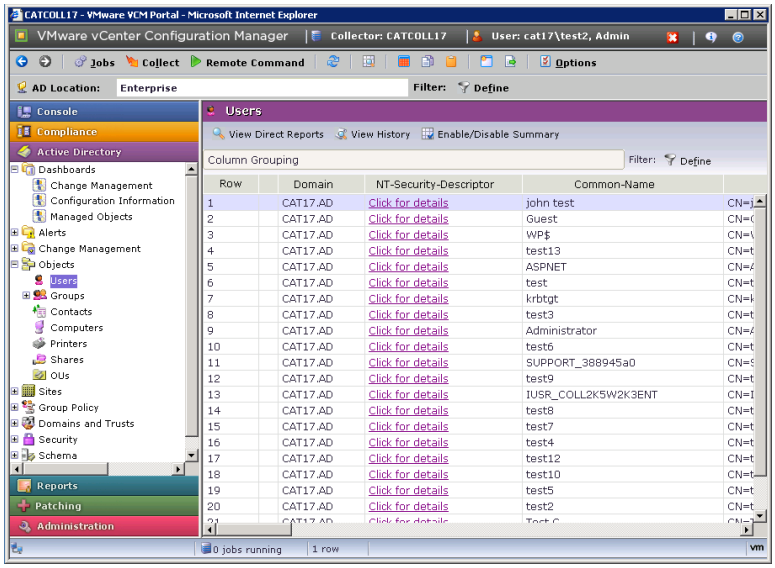
Note that several other Active Directory Dashboards are available. Take time to familiarize yourself with the remainder of the VCM for AD Dashboards.

Active Directory Summary Reports

Your AD Collection Results are also available to you in a more “raw” format as well. This level of reporting is more relevant for day to day operations, troubleshooting, and analysis and can be viewed in a Summary report or data grid format. To view a VCM for AD Summary report or data grid, click **Active Directory** | **Objects**. Select an object type.

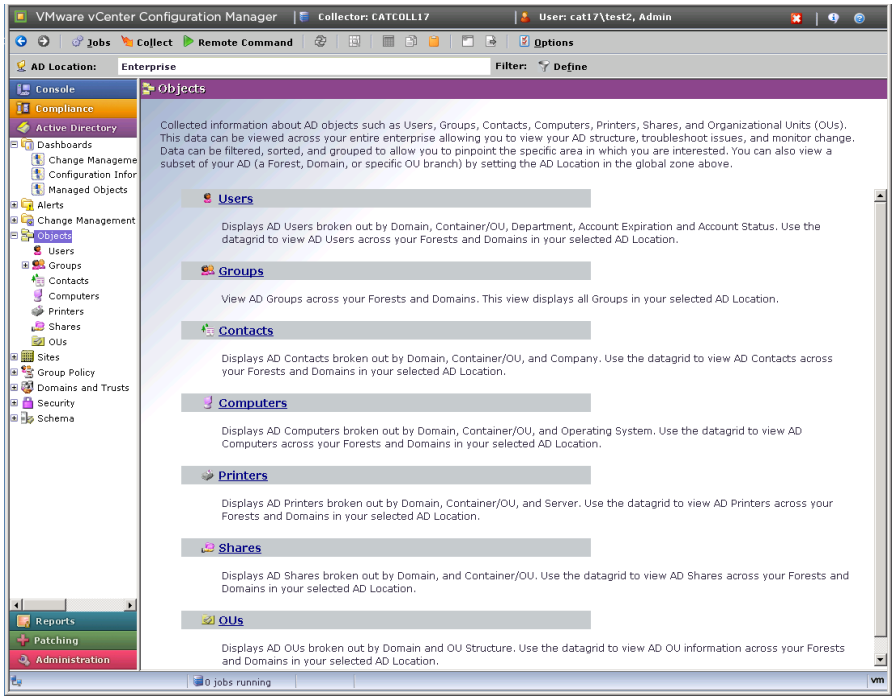


When you select the node, you will see a Summary Report, as displayed above, of the data you selected. Click **View Data Grid** to go directly to the data, or click an area of the Summary Report to filter the data before the data grid is displayed.



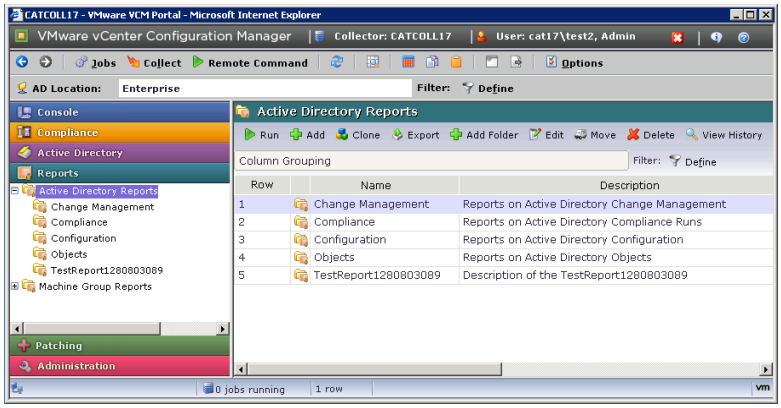
NOTE The default view is the Summary Report. At any time, however, you may switch the default view to go directly to the data grid by using the Enable/Disable Summary feature on the data grid view. See **Help** for more information on how to filter and sort your data and get full use of the data grid.

Several other categories (called “data classes”) of information regarding your AD Collection are available under the Active Directory Slider. This is where the remainder of your collected AD data is visible through the Portal.


VMware vCenter Configuration Manager
Collector: CATCOLL17
User: cat17\test2, Admin
Jobs
Collect
Remote Command
Options
AD Location:
Enterprise
Filter:
Define
Console
Compliance
Active Directory
Reports
Patching
Administration
Objects
Collected information about AD objects such as Users, Groups, Contacts, Computers, Printers, Shares, and Organizational Units (OUs). This data can be viewed across your entire enterprise allowing you to view your AD structure, troubleshoot issues, and monitor change. Data can be filtered, sorted, and grouped to allow you to pinpoint the specific area in which you are interested. You can also view a subset of your AD (a Forest, Domain, or specific OU branch) by setting the AD Location in the global zone above.
Users
Displays AD Users broken out by Domain, Container/OU, Department, Account Expiration and Account Status. Use the datagrid to view AD Users across your Forests and Domains in your selected AD Location.
Groups
View AD Groups across your Forests and Domains. This view displays all Groups in your selected AD Location.
Contacts
Displays AD Contacts broken out by Domain, Container/OU, and Company. Use the datagrid to view AD Contacts across your Forests and Domains in your selected AD Location.
Computers
Displays AD Computers broken out by Domain, Container/OU, and Operating System. Use the datagrid to view AD Computers across your Forests and Domains in your selected AD Location.
Printers
Displays AD Printers broken out by Domain, Container/OU, and Server. Use the datagrid to view AD Printers across your Forests and Domains in your selected AD Location.
Shares
Displays AD Shares broken out by Domain, and Container/OU. Use the datagrid to view AD Shares across your Forests and Domains in your selected AD Location.
OUs
Displays AD OUs broken out by Domain and OU Structure. Use the datagrid to view AD OU information across your Forests and Domains in your selected AD Location.
0 jobs running

Active Directory Reports

An alternative way to view your collected AD data is by running VCM Reports or creating your own custom reports using VCM's reporting wizard. To begin exploring VCM's Reporting functionality, click **Reports** | **Active Directory Reports**.



Like VCM for AD Dashboards, AD Reports are run real-time against the current data available in the CMDB, therefore they are only as current as of the time that the data was collected. In addition, it may require time for the report to generate based upon the volume or complexity of the data requested. Refer to the online Help for more information on how to schedule and disseminate reports.

Compliance for Active Directory

You may now begin to run Compliance against your collected data. To run a Compliance check, click the **Compliance** slider, and then follow the steps provided in the online Help to create rule groups, rules, filters, and templates.

Further Reading

Refer to Customizing VCM for information on how to customize for your environment. Each of these areas regarding customization also applies to VCM for Active Directory. You can also read "Maintaining VCM After Installation" on page 247 for important information regarding additional data retention settings and database maintenance steps which should be taken.

When using VCM for Active Directory, refer to the Help for specific task information. To access the Help, click the **Help** button, located on the Portal toolbar.

Getting Started with VCM for SMS 13

Getting Started with VCM for SMS

VCM for SMS provides continuous enterprise-wide OS, application, and security configuration management of all Microsoft SMS infrastructure components. By solving the issues associated with complex SMS installations, VCM for SMS integrates with SMS 2.0 and SMS 2003 to deliver an extensive solution for compliance monitoring, vulnerability assessment and remediation, change management, and software distribution.

VCM for SMS ensures that SMS will deliver consistent and accurate package installation by providing a comprehensive view of your organization's SMS infrastructure. In addition, the compliance engine in VCM for SMS detects, reports, alerts, and automatically remediates SMS client configuration drifts.

To begin using VCM for SMS, follow these steps.

1. Make VCM aware of your SMS Servers.
2. Perform SMS Server collections.
3. Perform SMS Client collections.
4. Explore VCM for SMS collection results.

Making VCM Aware of the SMS Servers

In order for your SMS Servers to be available for VCM collections, they must first be discovered and licensed in VCM. If you have already discovered and licensed these servers during your initial Discovery, proceed directly to "Performing SMS Server Collections" on page 228.

To determine whether your SMS Servers have been discovered and licensed, and are therefore available for SMS collections, follow these steps.

1. Click **Administration** | **Machines Manager** | **Licensed Machines** | **Licensed Windows Machines**. Scan the data grid to locate your SMS Servers.
   - If all SMS Servers that you want to manage are listed, and therefore licensed in VCM, proceed to "Performing SMS Server Collections" on page 228.
   - If you cannot locate your SMS Servers in this data grid, then they are not currently licensed. To determine whether they have been discovered and are available for licensing, proceed to the next step.
2. Click **Administration** | **Machines Manager** | **Available Machines** | **Available Windows Machines**. Scan the data grid to locate your SMS Servers.

- If all SMS Servers that you want to manage are listed, then they have been discovered; however, they must be licensed in order to make them available for SMS collections. Refer to "Licensing Windows Machines" on page 59 for instructions on how to license these machines.
- If you cannot locate your SMS Servers in this data grid, then they have not yet been discovered by VCM. You must first discover and license these machines before you can collect from them. Refer to "Discovering Windows Machines" on page 56, and then "Licensing Windows Machines" on page 59 for procedures on how to discover and license Windows machines.
- After your SMS Servers are discovered and licensed, proceed to "Performing SMS Server Collections" on page 228.

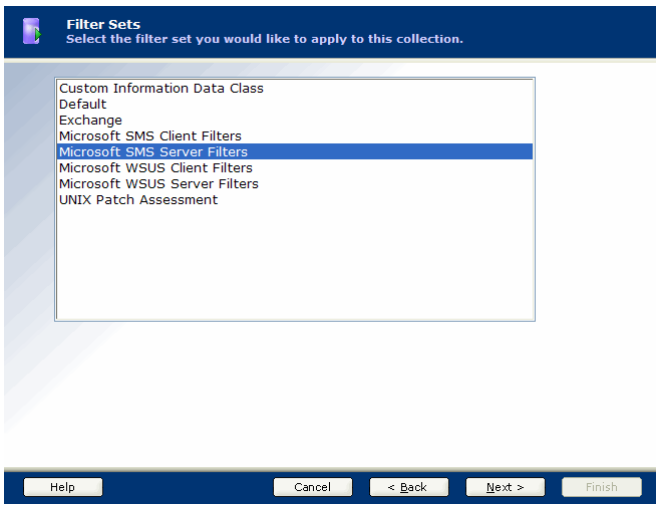
Performing SMS Server Collections

Now that you have verified that your SMS Servers are available and licensed in VCM, you must perform a VCM collection using the Microsoft SMS Server Filter set. This collection enables VCM to identify these machines as SMS Servers.

NOTE Before performing a collection on your SMS Servers, you should verify that the network authority account you are using has the appropriate SMS and WMI credentials to collect from those machines. If you are using an account that has permission to collect for VCM, but does not have permission to collect SMS or WMI information, you will not be able to collect and view the full range of data. For more information on Network Authority and VCM, refer to About Network Authority Settings in the online Help.

---

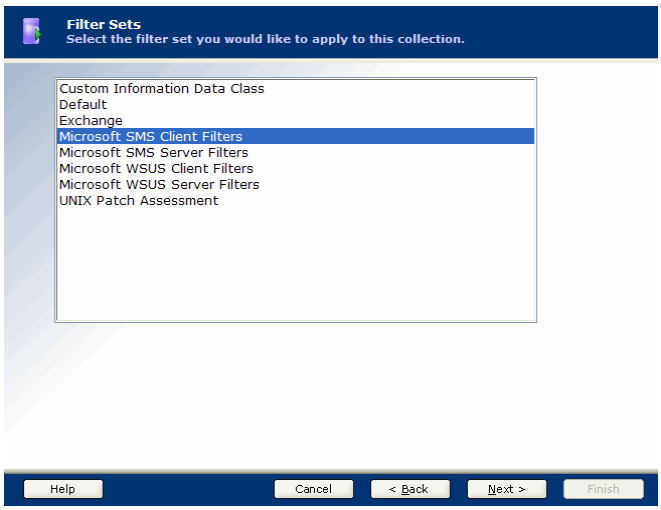
1. To perform a VCM collection, see the procedure described in "Performing an Initial Collection" on page 67.
2. Using this procedure, instead of selecting the default filter set, choose the **Select a Collection Filter Set to apply to these machines** option, and then select **Microsoft SMS Server Filters** from the **Filter Sets** list.



Performing SMS Client Collections

Now that your SMS Server Collection is complete, you must perform another collection using the **Microsoft SMS Client Filter** in order for VCM to collect SMS information from your SMS client machines. Once this collection is complete, you will be able to view all SMS Server and Client related data through VCM.

1. As with the SMS Server collection, use the procedure described in "Performing an Initial Collection" on page 67 to initiate your SMS Client collection.
2. Using this procedure, instead of selecting the default filter set, choose the **Select a Collection Filter Set to apply to these machines** option, and then select **Microsoft SMS Client Filters** from the **Filter Sets** list.



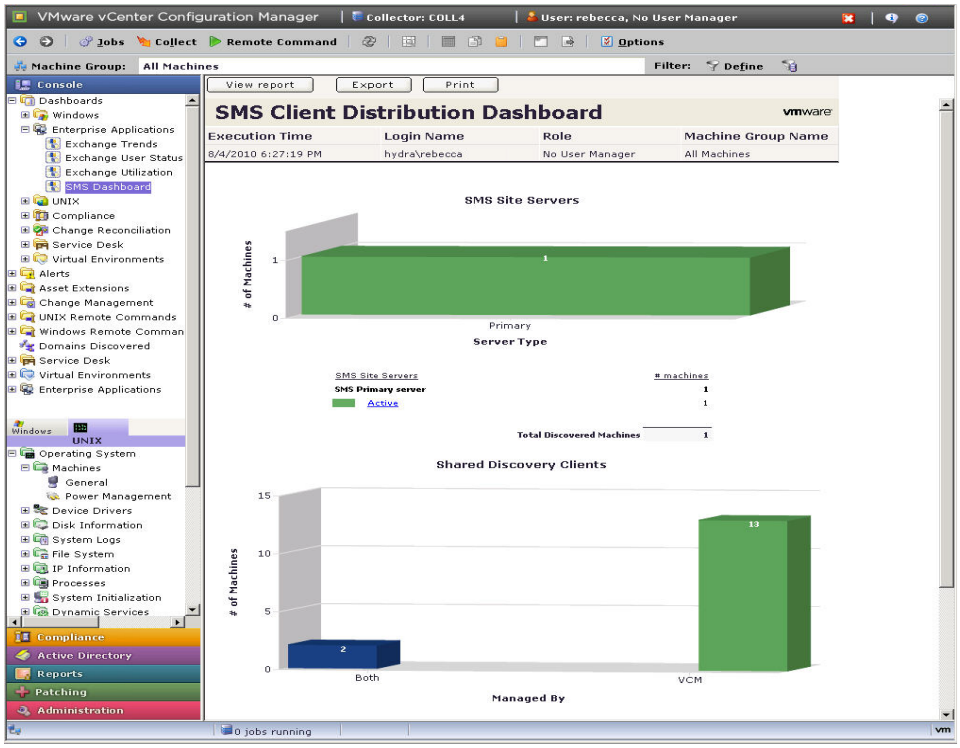
Exploring SMS Collection Results

After performing the initial SMS Server and Client collections, you can explore that data in the portal using the Console and Reports sliders.

Viewing SMS Dashboards

The SMS Dashboard contains information about your SMS Servers and Clients in a graphical format.

1. To view the SMS dashboard, select **Console | Dashboards | Enterprise Applications | SMS Dashboard**.

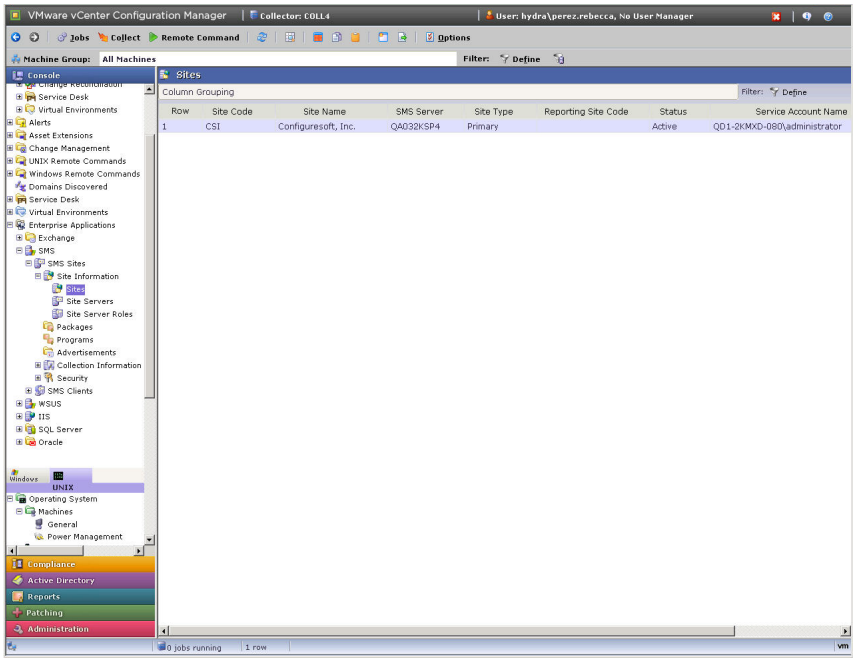


2. Click the **SMS Client** links or the **Chart bars** to drill down to detailed information on the machine or group of machines.

Viewing SMS Server Data

The Windows tab of the Console contains information about your SMS Server and Client machines.

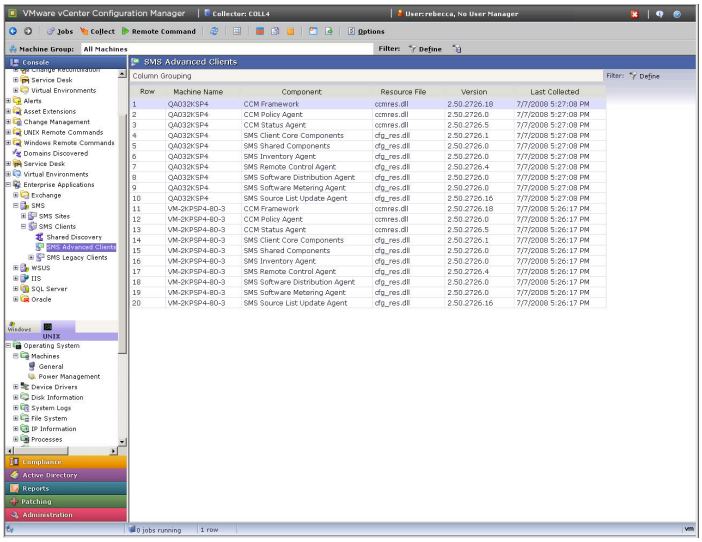
1. To view a list of your SMS Servers, along with additional information obtained during your initial SMS Server collection, select **Console** | **Enterprise Applications** | **SMS** | **SMS Sites** | **Site Information** | **Sites**.
2. View the list of Servers currently hosting SMS in the data grid.



Viewing SMS Client Data

The Windows tab of the Console contains information about your SMS Clients.

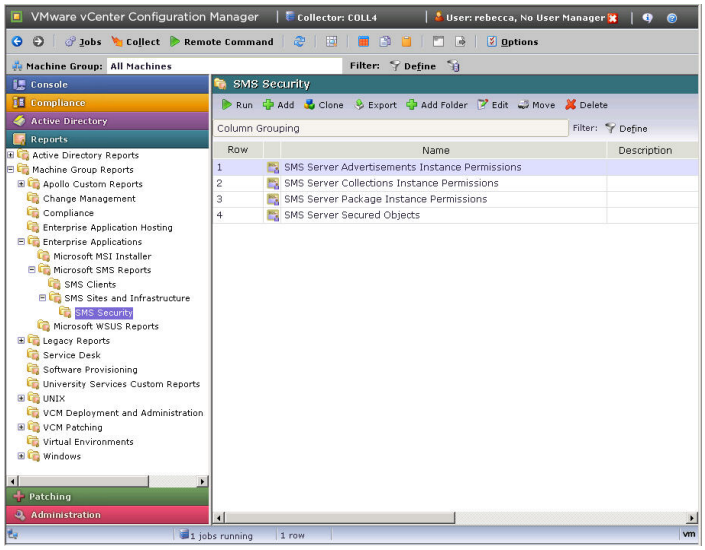
1. To view a list of your SMS Clients, select **Console | Windows (tab) | Enterprise Applications | SMS | SMS Clients | SMS Advanced Clients**.
2. View the SMS client machines in the data grid, along with details about the SMS component they contain, the Resource file, and Version number.



Viewing SMS Reports

An alternative way to view your collected SMS data is by running Reports, or by creating your own custom reports using VCM's reporting wizard.

1. To begin exploring VCM's Reporting functionality, select **Reports** | **Machine Group Reports** | **Enterprise Applications** | **Microsoft SMS Reports**.



2. View the SMS report data in the data grid. As with the **VCM for SMS Dashboard**, Reports are run against the current data available in the CMDB. Therefore, they are current only as of the time when the data was collected. In addition, it may require time for the report to generate based upon the volume or complexity of the data requested. For more information on how to schedule and disseminate reports, see the online Help.

You may now begin to check Compliance on your collected data by creating rule groups, rules, filters, and templates. See About Compliance in the online Help.

Further Reading

Refer to "Customize VCM for your Environment" on page 115 for information on how to customize for your environment. Each of these areas regarding customization also applies to VCM for SMS. Also read about maintaining VCM after installation in "Maintaining VCM After Installation" on page 247 for important information regarding additional data retention settings and database maintenance steps that should be taken.

When using VCM for SMS, refer to the Help for specific task information. To access the Help, click the **Help** button on the toolbar.

Getting Started with Windows Server Update Services 14

Getting Started with Windows Server Update Services

VCM for Windows Server Update Services (VCM for WSUS) provides continuous enterprise-wide OS, application, and security configuration management of Microsoft WSUS client components.

To use VCM for WSUS, follow these steps.

1. Make VCM aware of your WSUS Servers.
2. Perform WSUS Server collections.
3. Perform WSUS Client collections.
4. Explore WSUS collection results.

Making VCM Aware of the WSUS Server

In order for your WSUS Servers to be available for VCM collections, they must first be discovered and licensed in VCM. If you have already discovered and licensed these servers during your initial Discovery, you can proceed directly to "Performing WSUS Server Collections" on page 236

To determine whether your WSUS Servers have been discovered and licensed, and are therefore available for WSUS Collections, follow these steps.

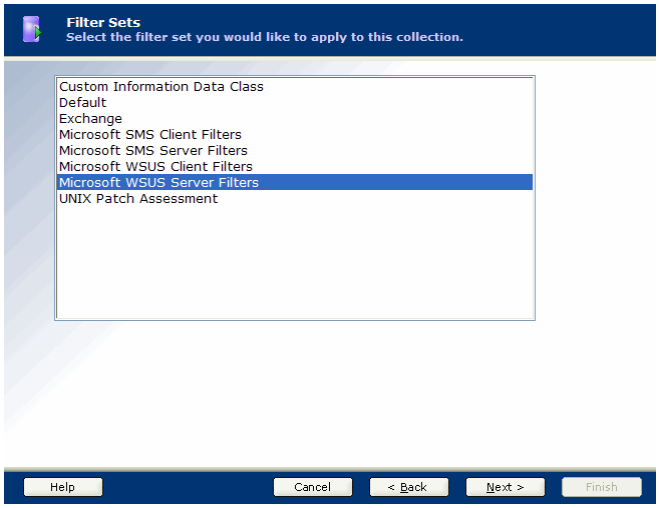
1. Click **Administration | Machines Manager | Licensed Machines | Licensed Windows Machines**. View the data grid to locate your WSUS Servers.
   - If all WSUS Servers that you want to manage are present in VCM, and therefore are licensed, proceed to "Performing WSUS Server Collections" on page 236.
   - If you cannot locate your WSUS Servers in this data grid, they are not currently licensed. To determine whether they have been discovered and are available for licensing, proceed to the next step.
2. Click **Administration | Machines Manager | Available Machines | Available Windows Machines**. View the data grid to locate your WSUS Servers.
   - If all WSUS Servers that you want to manage are present, they have been discovered, but must be licensed in order to make them available for WSUS collections. Refer to "Licensing Windows Machines" on page 59 for instructions on how to license these machines.

- If you cannot locate your WSUS Servers in this data grid, they have not yet been discovered by VCM. You must first discover, and then license these machines before you can collect from them. Refer to "Discovering Windows Machines" on page 56, and then "Licensing Windows Machines" on page 59 for instructions on how to discover and license Windows machines. After your WSUS Servers are discovered and licensed, proceed to "Performing WSUS Server Collections" on page 236.

Performing WSUS Server Collections

Now that you have verified that your WSUS Servers are available and licensed in VCM, you must perform a collection using the Microsoft WSUS Server Filter set. This collection will enable VCM to identify these machines as WSUS Servers.

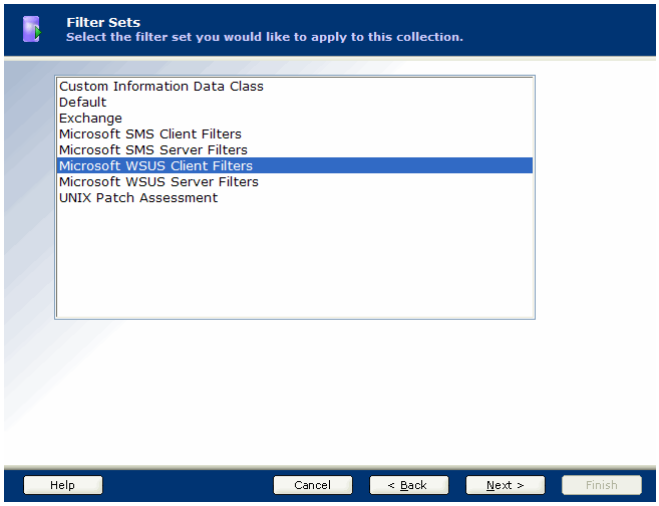
1. To perform a VCM collection, see the procedure described in "Performing an Initial Collection" on page 67.
2. Using this procedure, instead of selecting the default filter set, choose the **Select a Collection Filter Set to apply to these machines** option, and then select **Microsoft WSUS Server Filters** from the **Filter Sets** list.



Performing WSUS Client Collections

Now that your WSUS Server Collection is complete, you must perform another collection using the Microsoft WSUS Client Filter in order for VCM to collect WSUS information from your WSUS client machines. Once this collection is complete, you will be able to view all WSUS Server and Client related data through VCM.

1. As with the WSUS Server collection, use the procedure described in "Performing an Initial Collection" on page 67 to initiate your WSUS Client collection.
2. Using this procedure, instead of selecting the default filter set, choose the **Select a Collection Filter Set to apply to these machines** option, and then select **Microsoft WSUS Client Filters** from the **Filter Sets** list.

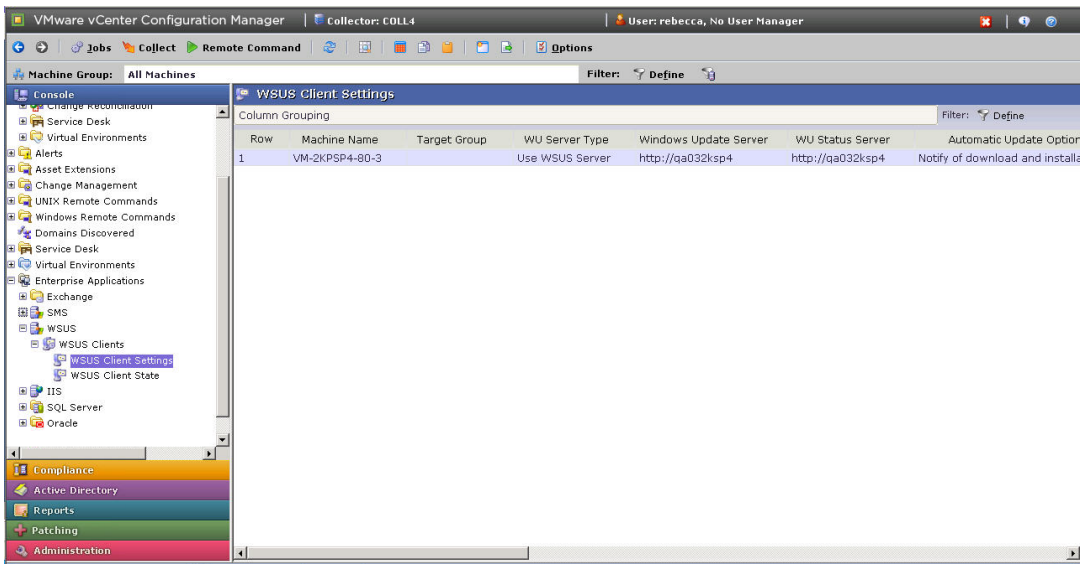


Exploring WSUS Collection Results

After performing initial WSUS Server and Client collections, you can explore that data in the portal using the Console and Reports sliders.

Viewing WSUS Clients

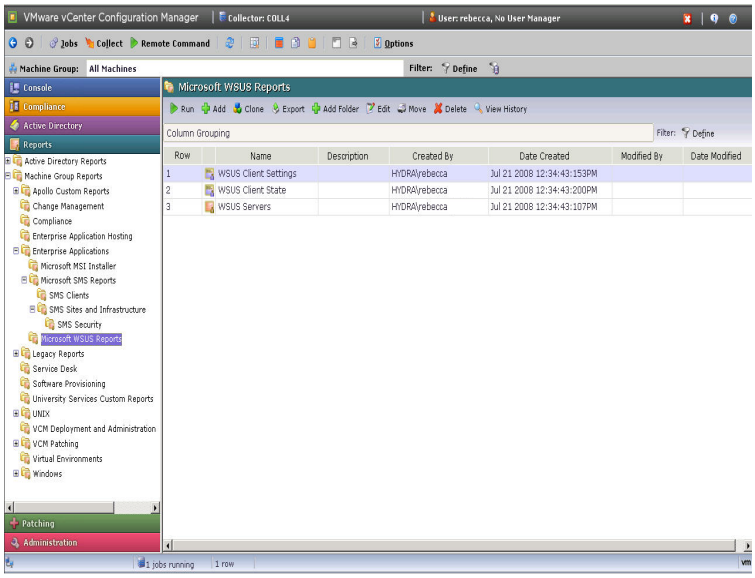
To view information about your WSUS Clients, click **Console** | **Enterprise Applications** | **WSUS** | **WSUS Clients** | **WSUS Client Settings**.



Viewing WSUS Reports

In addition to using Reports to view your WSUS Server data, you can also run Reports to view data about your WSUS Client Settings and WSUS Client State.

1. To view information about your WSUS Servers, click **Reports** | **Machine Group Reports** | **Enterprise Applications** | **Microsoft WSUS Reports**.
2. Select **WSUS Servers**, and then click **Run**. The report lists your WSUS Servers and other information about those machines.



VCM for WSUS Reports are run against the current data available in the CMDB, and therefore are only as current as the last time that the data was collected. In addition, it may require time for the report to generate based upon the volume or complexity of the data requested. For more information on how to schedule and disseminate reports, see the online Help.

You may now begin to check Compliance on your collected data by creating rule groups, rules, filters, and templates. See About Compliance in the online Help.

Further Reading

Refer to "Customize VCM for your Environment" on page 115 for information on how to customize for your environment. Each of these areas regarding customization also applies to VCM for WSUS. Also read about maintaining VCM after installation in "Maintaining VCM After Installation" on page 247 for important information regarding additional data retention settings and database maintenance steps that should be taken.

When using VCM for WSUS, refer to the Help for specific task information. To access the Help, click the **Help** button on the toolbar.

Accessing Additional Compliance Content 15

VMware provides several additional VCM Compliance Content Packages relative to the different components you have just activated. These packages are not available in the Portal until you download and import them. It is important to check to see if any of the VCM Compliance Content Packages are important to your organization, and then import them at this time.

Before you begin using this content, you must complete the following required steps:

1. Locate the Content Directory.
2. Launch VMware Compliance Content Wizard (CCW) to Import Relevant Content.
3. Explore Imported Content Results in the Portal.

Locating the Content Directory

To access the Content Packages that were supplied during your VCM content download, navigate to: **C:\Documents and Settings\All Users\Application Data\Configuresoft\ECMImportExport\Content**.

Launching the Content Wizard to Import Relevant Content

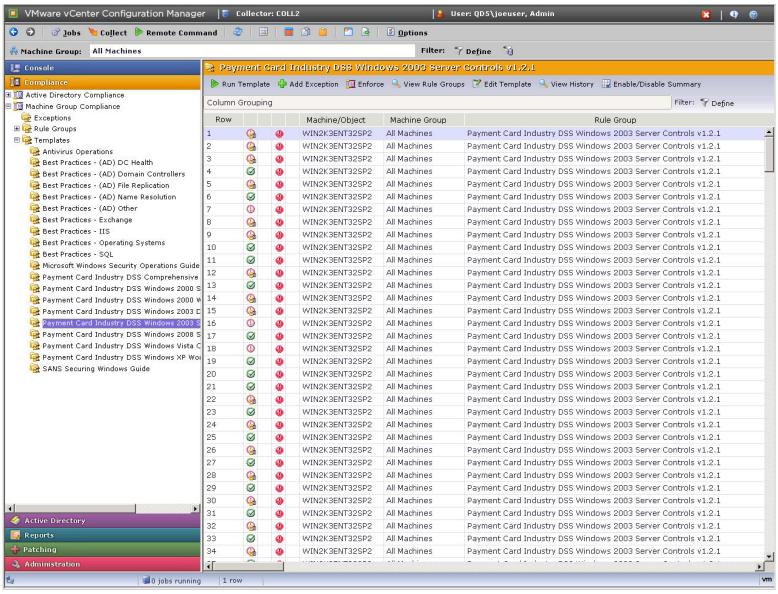
If you are loading content into VCM for the first time, refer to Section 15.4: VCM Import/Export and VMware Content Wizard for information on how to launch VMware Content Wizard. Once you have performed this initial load, you can maintain your content with VMware VCM Import/Export.

NOTE If you have Internet connectivity from your Collector, you may use the VMware Content Wizard to browse to the latest content and download it directly from VMware. VMware Content Packages are updated frequently and new Content Packages are released on a regular basis. Regardless of your connectivity, VMware recommends that you check back regularly for content updates.

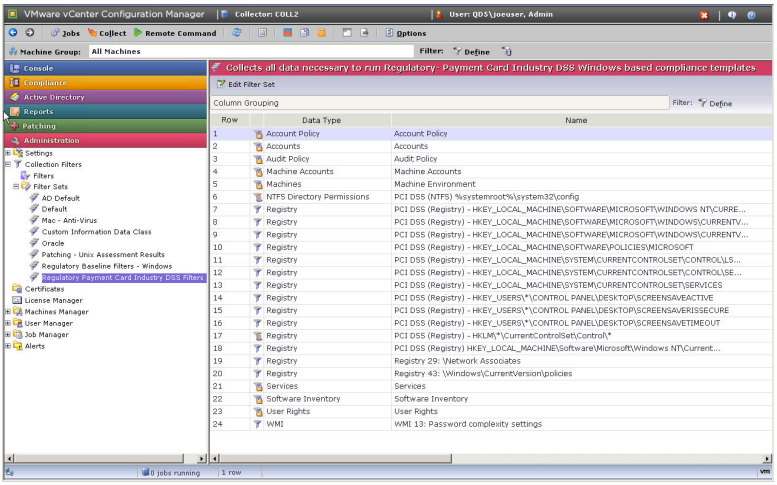
Exploring Imported Content Results in the Portal

Depending upon the particular VCM Content Package(s) you have imported, the results of your import will appear in the Portal in the following locations, with their rules and rule groups expanded beneath the corresponding Compliance nodes.

- **Compliance | Machine Group Compliance | Templates**
- **Compliance | Active Directory Compliance | Templates**



If the particular Content Package(s) you have imported contains filter sets, they will appear under **Administration | Collection Filters | Filter Sets**.



Particular VCM Content Package(s) may contain SSRS Reports, SSRS Node Summaries, and SSRS Dashboards, which will show up in their respective locations in the Portal.

Once this content has been imported into the Portal, further collections using custom filters may be required to use it. These are included in the Content Package. Refer to the online Help for information on how to use a custom filter set. Once the appropriate data has been collected relevant to the Content Package, refer to the online Help to learn more about running Compliance Templates.

Installing and Getting Started with VCM Tools

16

All VCM components and tools were automatically installed on the Collector machine by the VCM Installation Manager during installation, as explained in the chapter Using VCM Installation Manager. However, if you want to install only the VCM tools on a non-Collector machine, follow the procedure in the first section in this chapter, Installing the Tools Only.

The subsequent sections in this chapter explain how to get started using the VCM tools, including:

- Foundation Checker
- Job Manager Tool
- Import/Export and Content Wizard

Installing the VCM Tools Only

If you want to install only the VCM tools on any Windows machine other than the Collector, follow the procedure in this section. If you will later be installing VCM on this machine, you will first need to uninstall these tools and then install VCM.

1. Insert the installation CD into a drive on the non-Collector machine on which you want to install the tools. The **Installation Manager** appears.
2. Click **Run Installation Manager**.
3. Complete the initial pages, clicking **Next** to move to each subsequent page, until the **Select Installation Type** screen appears.
4. On the **Select Installation Type** page, select the **Advanced Installation** check box, and then select **Tools**.
5. Clear the **VMware vCenter Configuration Manager** check box.
6. To install all of the tools, leave **Tools** checked, which will leave all of the individual tools checked as well. To install a subset of the tools instead, clear the Tools check box, and then clear the check box for each tool you do not want to install. (That is, only the tools you want to install are selected..)
7. Click **Next**.
8. Complete the remaining screens, clicking Next to move to each subsequent screen, until the **Installation Complete** page appears.
9. Click **Finish**. You return to the initial Installation page of the Installation Manager. Click **Exit** to close the Installation Manager.

The VCM tool or tools are now installed on this machine. Proceed to the following sections in this chapter to get started using the tools.

NOTE The VCM Tools installation has prerequisites much like a VCM installation. Each tool in the Advanced Installation has its own installation requirements. For example, Import/Export (I/E) and Content Wizard cannot be installed on a machine that is not running VCM, and Job Manager requires .NET. Because of these requirements, you should specifically select the tools that you want to install, and note the installation requirements that VCM Installation Manager confirms using Foundation Checker.

Foundation Checker

Installation Manager uses VCM Foundation Checker to check a machine's viability for a successful VCM deployment. Foundation Checker runs a series of system checks that look for various conditions, settings, and requirements. Once the system checks are complete, a results file lists which system checks passed, failed, or generated warnings.

When system checks fail, the results file includes remediation steps describing how to fix the conditions that caused the system checks to fail (a failed condition is indicated with an Error status). After you fix the conditions, you can run Foundation Checker again to ensure that all of the remediation steps were successful. If you encounter issues with your configuration, contact VMware Customer Support. A Team member may ask you to run Foundation Checker and confirm the configuration results.

Installation Manager also installs a command line version of Foundation Checker on your Collector machine during installation. For more information, see the *Foundation Checker User's Guide* in C:\Program Files\VMware\VCM\Documentation.

Once you have launched Foundation Checker, follow the steps in the wizard.

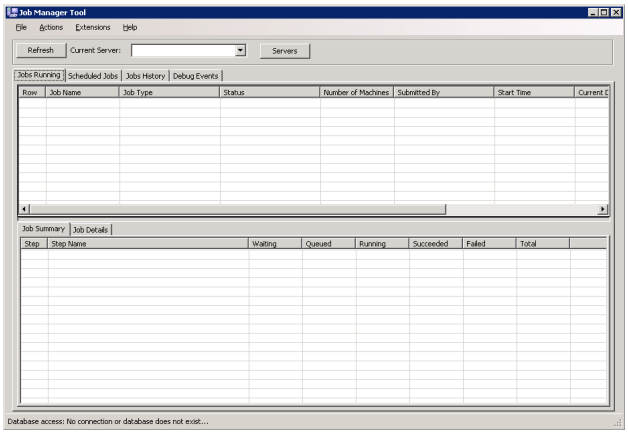
IMPORTANT If you choose to install and run the Foundation Checker before installation, it is important to uninstall the Foundation Checker before running the Installation Manager.

VCM Job Manager Tool

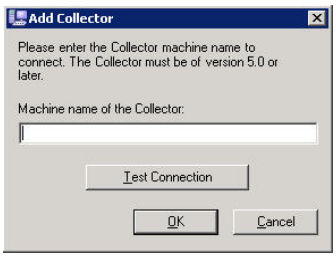
Use the Job Manager tool to view the status of VCM jobs that are currently running or are scheduled to run on one or more collectors. In addition, you can use the tool to view the history of completed jobs. Job types that can be viewed and scheduled include collections, discoveries, reports, compliance template runs, agent installations, and console change actions. You can run the Job Manager Tool on a machine, separate from your Collector machine, to manage jobs without launching the VCM Portal.

The Job Manager tool was automatically installed on your Collector machine during your installation. If you want to install the Job Manager tool on a non-Collector machine, see Installing and Getting Started with VCM Tools .

1. To start the Job Manager Tool, click **Start | All Programs | VMware vCenter Configuration Manager | Tools | Job Manager Tool**.



2. When you launch the Job Manager Tool the first time, you must add your VCM Collectors before you can view any job data originating from those machines. Click the **Servers** button, located below the menu bar. The **Add Collector** dialog box appears.


Add Collector
Please enter the Collector machine name to connect. The Collector must be of version 5.0 or later.
Machine name of the Collector:
Test Connection
OK
Cancel

3. Type the machine name of your Collector in the **Machine name of the Collector** text box.
4. Click **Test Connection** to verify that your connection is valid. If your connection is successful, you will see the following message: **Database connection test Succeeded**. If it is unsuccessful, an error message will appear with details specific to the connection failure. Resolve the connection failure, and then repeat these steps until you receive a success message.
5. Click **OK**. Your VCM database server is now added to the list of servers.

NOTE To edit this list at any time, click the **Servers** button again to access **Server Manager**.

6. Click the **Refresh** button update the displayed job information with any data now available from the server to which you just connected.

NOTE Once a valid server is added, it automatically appears in the **Current Server** drop-down list. Each time you start Job Manager, it attempts to connect to the server used last during hte previous session. If this server cannot be contacted, an error message appears and further attempts to contact that machine cease. To force another connection attempt, click **Refresh**. If more than one server is in the list, then changing servers will trigger a connection attempt for the newly selected server. For more information on how to use Job Manager, click **Help | Contents**.

VCM Import/Export and Content Wizard (CW)

Use Import/Export (I/E) and the Content Wizard (CW) to move or update VCM Business Objects between databases. These tools do not import or export any collected data. However, they support the migration of any VCM Management Extension for Asset data that has been added to VCM manually. Specifically, the Import/Export Tool supports the following scenarios:

- Backup (export) and restore (import) Business Objects to the same machine.
- Backup (export) and import (if needed) Business Objects during a VCM upgrade.
- Export and migrate (import) Business Objects to additional machines in a multi-Collector environment (during setup or to move custom content).
- Using CW, download current Compliance Content from VMware and import it into an existing database • Using the Command Line Interface, automate the propagation of content to other machines in a multi-collector environment with a “Golden Machine”.
- Aid in disaster recovery using the Command Line Interface to automate and schedule the backup of VCM content and configuration parameters.

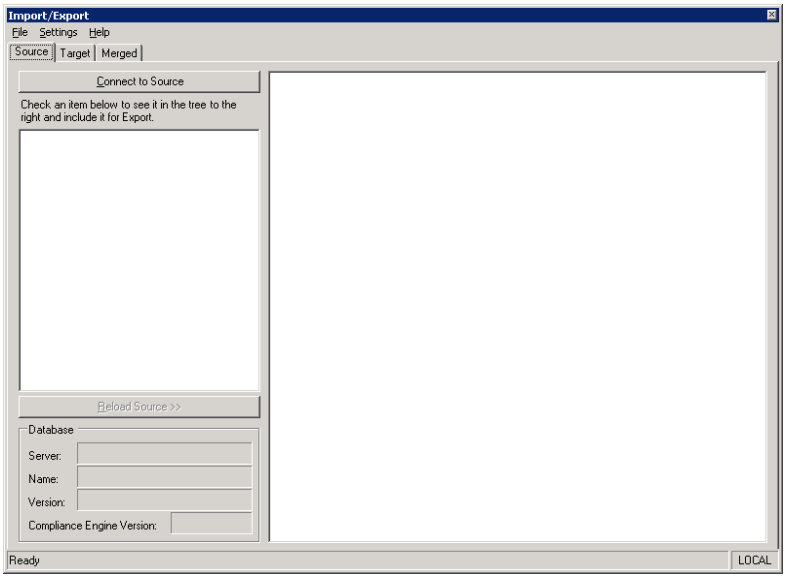
The Command Line Interface (CLI) is a powerful extension of the Import/Export graphic user interface (GUI). In addition to supporting the scenarios noted above, the CLI allows content to be overwritten (as opposed to “rename only”) and provides for automation through scripting suitable for customizations.

IMPORTANT Use of the CLI should be restricted to advanced users who exercise caution when testing out their scripts.

Import/Export and CW were automatically installed on your Collector machine during your VCMinstallation. Import/Export and CW can only be run on a Collector machine. Refer to the following sections to get started with each tool.

VCM Import/Export

1. To start Import/Export on your Collector machine, click **Start | All Programs | VMware vCenter Configuration Manager | Tools | Import Export Tool.**



2. To use Import/Export, you must identify a source for the data to be imported or exported. Click Connect to Source (or Connect to Target, if you are exporting). The Connect to Data Store dialog box appears.
3. If you are importing, you can either select a **Server** in the drop-down list or type a server name in the text box, or import VMware content supplied by Installation Manager. To import content, click the ellipses button (...) to the right of the **File** text box, and then browse to the appropriate Content Package, commonly located at: C:\Documents and Settings\All Users\Application Data\CM\Content\.

NOTE To add a new database, enter the database name into the selection field.

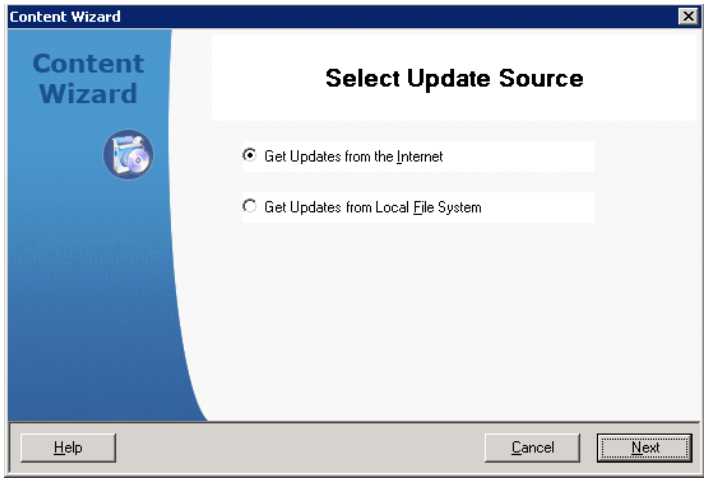
4. Identify a Target (destination) for the data to be exported from within the Target tab. The target identifies the database to be imported into or compared with, or an xml file to be imported into or compared against.
5. If importing to a database, compare the selections made on the Source tab with the Target database. Specifically, you can compare the names of items and elements selected on the Source tab with the corresponding names of items and elements in the target database. Any duplicate items and elements must be resolved before you can continue with the import operation.

For detailed procedures on any of these steps, click **Help** | **Contents**, then select the appropriate topic from the left Table of Contents pane.

NOTE We recommend that you refer to Import/Export Help to gain a thorough understanding of the logging of Content that is not imported by Import/Export even though it is requested by the user.

Content Wizard

Unlike Import/Export, Content Wizard may be used when no user intervention is required or when you want to connect directly to the VMware website for the latest Content Package updates. To start the CW from your Collector Machine, click **Start** | **All Programs** | **VMware vCenter Configuration Manager** | **Tools** | **Content Wizard**.



Before you can use Content Wizard, you must specify whether you want to **Get Updates from the Internet** (which requires Internet connectivity and access beyond your local network) or **Get Updates from Local File System** if you would like to select a Content Package supplied by VCM Installation Manager. If you choose local file system, CW automatically looks in the previously mentioned Content folder. You cannot browse to an alternate location.

As you proceed through the wizard, you can select which content packages you want to import. Be advised that some Content Packages are very large. Therefore, in order to maximize performance and reduce the possibility of encountering a network issue impacting the download and/or import process, we recommend that you subdivide your imports to no more than two to three packages at a time.

Follow the wizard to completion. Since the Import/Export Merge process is transparent to the user when using CW, you must refer to the error log for any issues regarding the download or import process.

Maintaining VCM After Installation 17

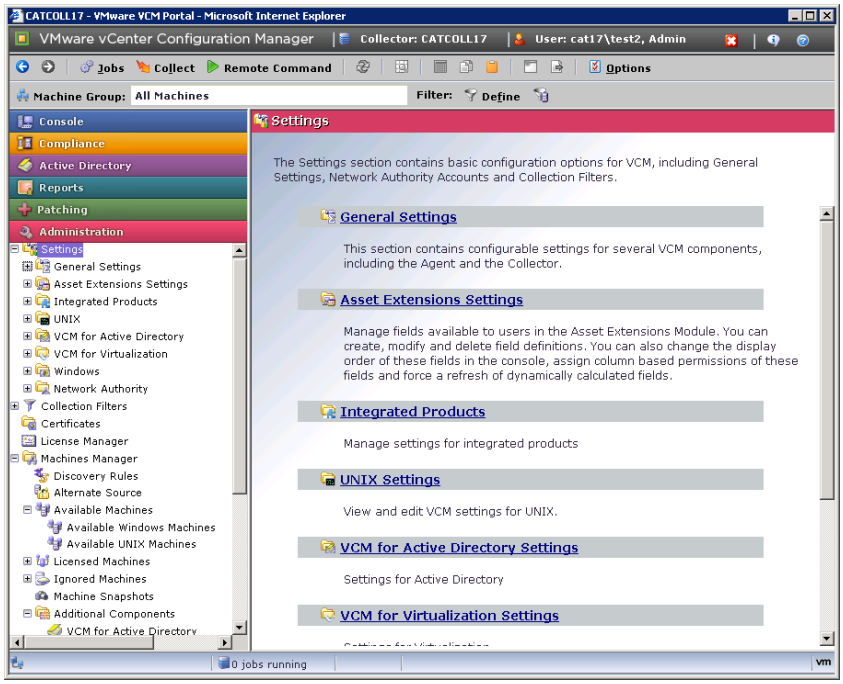
Once you have performed initial setup and familiarized yourself with VCM and its components and tools, VMware recommends you step through the specific configuration settings for each licensed component and customize them. Additionally, you should perform routine maintenance on your VCM CMDB just as you would any other SQL database in your enterprise.

Follow the guidance below to keep VCM running smoothly and performing efficiently.

1. Customize VCM and component-specific settings.
2. Configure Database file growth.
3. Configure Database recovery settings.
4. Create a Maintenance Plan for SQL Server 2005.
5. Incorporate the VCM CMDB into your backup/disaster recovery plans.

Customize VCM and Component-specific Settings

VCM and its components have several configuration settings that should be customized to your environment. VMware strongly suggests reviewing **Administration | Settings** to familiarize yourself with the configuration parameters that should be customized to your environment. In addition, you should specify settings such as data retention and thread priorities for communication with the agent for certain collection types.



In addition to several general global settings, the following components also have specific settings that should be considered if you have licensed that particular component.

- Asset Extensions (VCMMXA)
- VCM for Active Directory
- VCM for Virtualization
- UNIX
- Windows

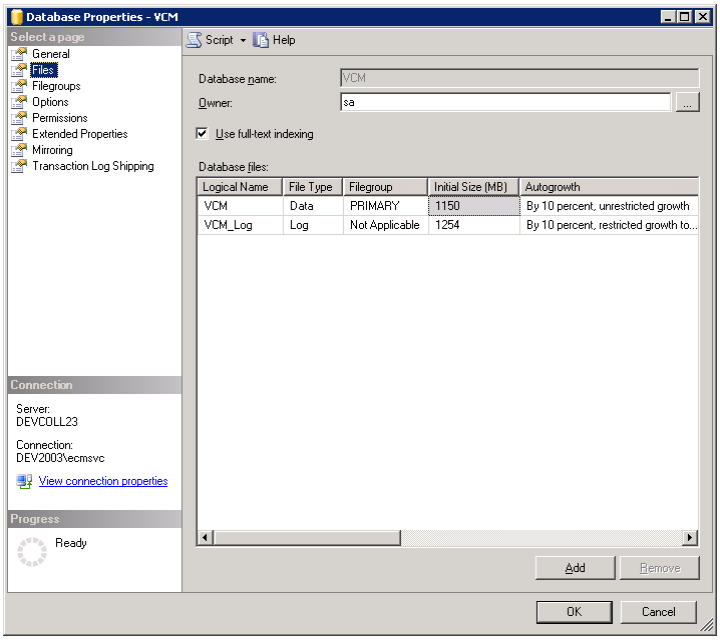
For more information on settings specific to those products, refer to the Help associated with each product. To access the Help for any particular Component, navigate to a node within that Component, and then click **Help**.

Configure Database File Growth

After VCM is installed, the installer creates a single 250 MB data file and a 25 MB log file. As data is added to VCM through normal operations, these files will grow as required. Unfortunately, the growth settings are set to default, which can easily cause fragmentation in the files. It is important to set the **AutoGrowth** setting properly in each of the databases.

In the **Automatically grow** file section, select **By percent** and make sure this setting is at least **10%**. This setting should be configured on each VCM-related database.

1. Select **Start | All Programs | Microsoft SQL Server 2005 | SQL Server Management Studio**. Connect to the Microsoft SQL Server Management Studio.
2. Expand the SQL instance.
3. Expand **Databases**.
4. Right-click **VCM** and select **Properties**. The **Database Properties** window appears.



5. In the left pane, select **Files**. The right pane displays VCM and VCM_Log.
6. In the **Autogrowth** column, click the ellipsis button. The **Change Autogrowth for VCM** dialog box appears.
7. Select **Enable Autogrowth**.
8. In the **File Growth** area, select and type or select 10 or greater in the text box. This setting indicates that every time the transaction log file grows, it will grow by 10% of its current size. This setting is very critical in larger environments where the log file can grow large even when using the Simple recovery model. If possible, reserve as much space as possible for your transaction log file so that it does not ever have to grow. This configuration will result in the best performance.
9. In the **Maximum File Size** area, select **Unrestricted Growth**.
10. Click **OK** to save and close the dialog box.
11. Repeat the same procedures for **VCM_Log**.
12. Return to the database list and repeat the above procedures for all VCM-related databases.

Configure Database Recovery Settings

SQL Server supports the following individual "Recovery Models" in SQL Server. They can be set differently for each database. They are:

- **Simple:** In Simple recovery, the only information kept in the transaction log is data that is necessary to recover the database to a known good state when the server restarts. It is a misconception that this setting does not cause the transaction log file to grow. In this mode, SQL Server is in what is known as "Auto Truncate" mode, which means that the log file is periodically "rolled over" as data is moved from the log file to the data file. In this mode, transaction log backups are not allowed, and "point in time" recovery is not available. Due to the nature of VCM, it is recommended that the Simple recovery model be used for all VMware databases, and that nightly FULL or INCREMENTAL backups be used.
- **Bulk Logged:** In Bulk Logged recovery, the transaction log retains all "normal" transaction information, and effectively discards those that result from a bulk operation. VCM makes extensive use of the IROWSETFASTLOAD interface, which is bulk logged.
- **Full:** In Full recovery, the transaction log retains all information until it is effectively purged through the use of a SQL Server LOG backup operation. This setting is used when the Database Administrator wants to be able to perform point in time recovery. It is also used to allow incremental backups of the database. In VCM, there are other factors involved that make point in time recovery at best, tenuous. It is recommended that you do not use this model. If you do decide to implement Full Recovery it is critical to set up scheduled (generally daily) backups of the transaction log. The log files will continue to grow and accumulate changes until they are backed up, so a Full Recovery database without scheduled backups can quickly fill its disk and stop the system.

NOTE VCM database settings are set to Simple by default. If you change the VCM database recovery setting to Full, you must manage your own log backups.

To configure the database recovery settings, follow these steps:

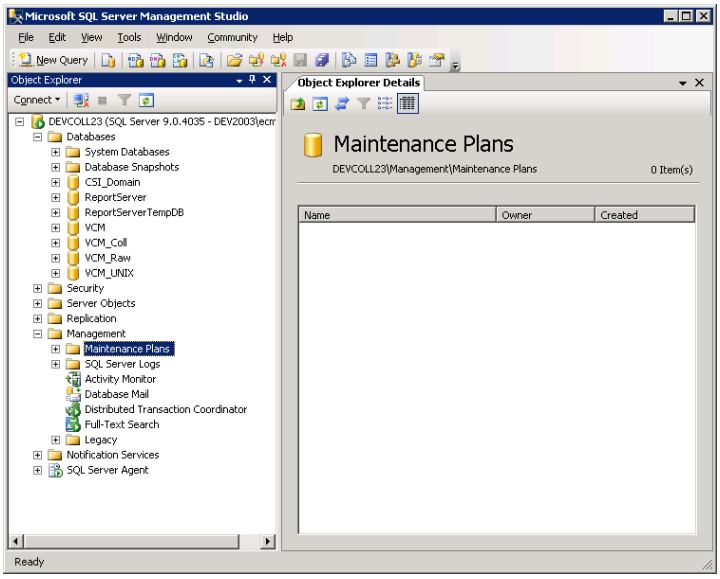
- Connect to the Microsoft SQL Server Management Studio by selecting **Start | All Programs | Microsoft SQL Server 2005 | SQL Server Management Studio**.
- Expand the **SQL instance**.
- Expand **Databases**.
- Right-click **VCM** and select **Properties**. The Database Properties dialog box appears.
- In the upper-left pane, click **Options**. The options pane appears.
- In the Recovery model drop-down, select either **Simple**, **Bulk-logged**, or **Full**. Click **OK** to close the Database Properties dialog box.

Create a Maintenance Plan for SQL Server 2005

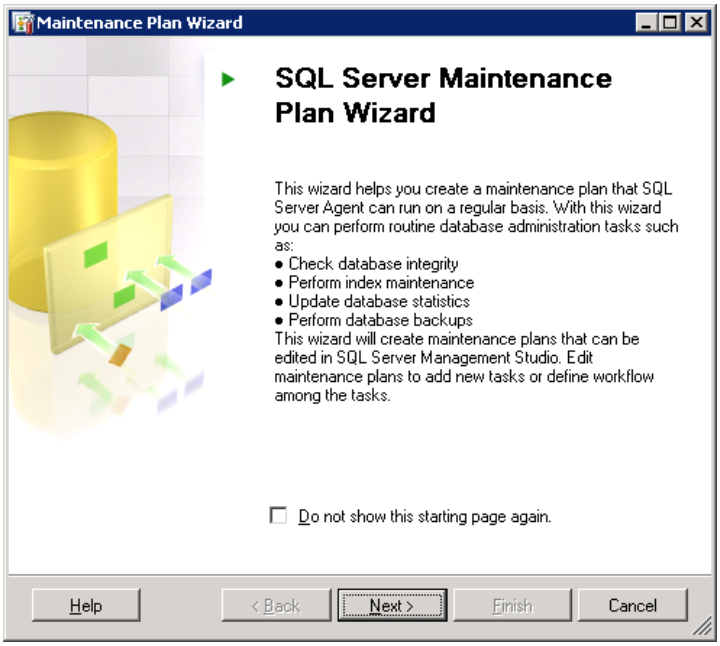
Because VCM relies heavily on its SQL databases for its operation, SQL Server 2005 should undergo routine maintenance. By setting up the automated maintenance functions on SQL 2005 servers hosting the VCM database, VCM will run at peak performance and should require little operator intervention during its lifecycle.

Follow these steps to create a maintenance plan for SQL Server 2005.

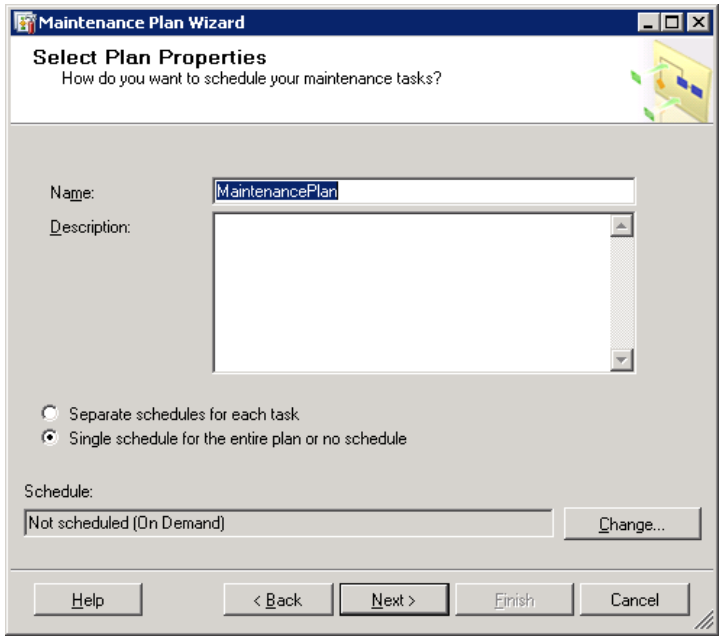
1. Start Microsoft SQL Server Management Studio.



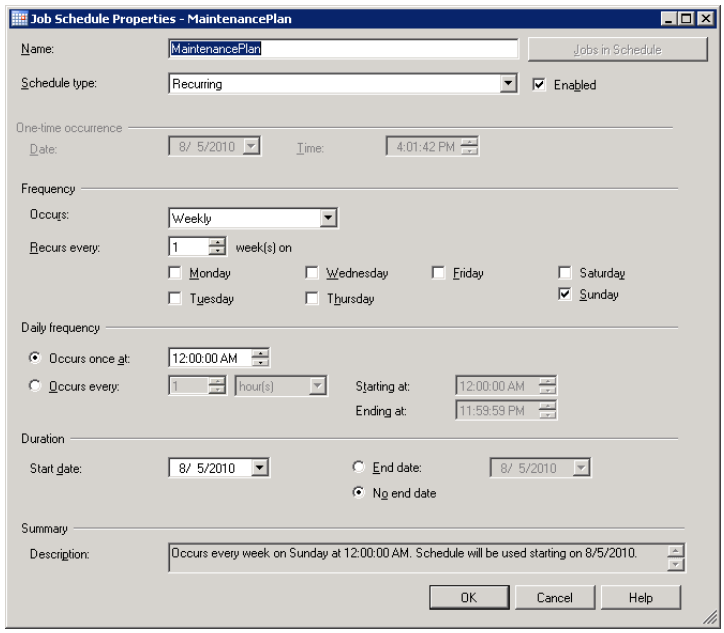
2. Open the **Management** folder, right-click **Maintenance Plans**, and then select **Maintenance Plan Wizard**. The SQL Server Maintenance Plan Wizard opens.


Maintenance Plan Wizard
SQL Server Maintenance Plan Wizard
This wizard helps you create a maintenance plan that SQL Server Agent can run on a regular basis. With this wizard you can perform routine database administration tasks such as:
• Check database integrity
• Perform index maintenance
• Update database statistics
• Perform database backups
This wizard will create maintenance plans that can be edited in SQL Server Management Studio. Edit maintenance plans to add new tasks or define workflow among the tasks.
Do not show this starting page again.
Help
< Back
Next >
Finish
Cancel

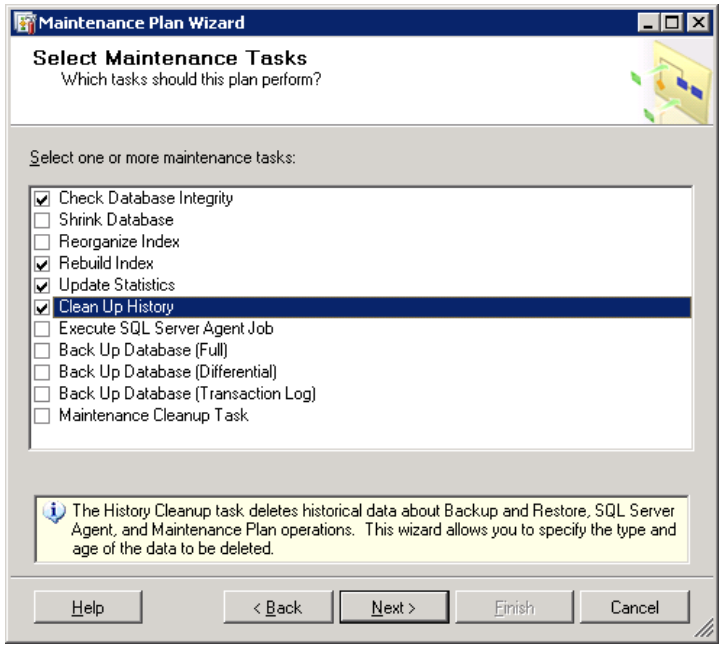
3. Click **Next**. The Select Plan Properties page appears.



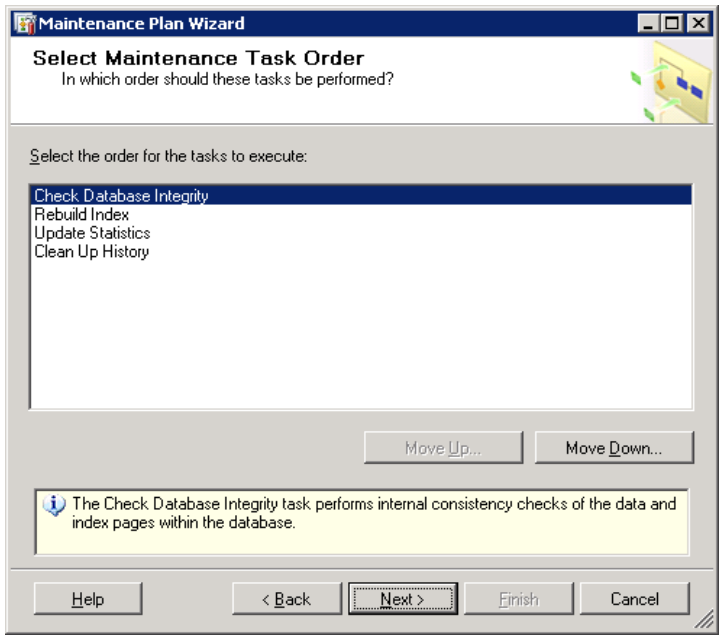
4. Enter a maintenance plan name, and then select **Single schedule for the entire plan or no schedule**. Click **Change**. The Job Schedule Properties - Maintenance Plan dialog box appears.



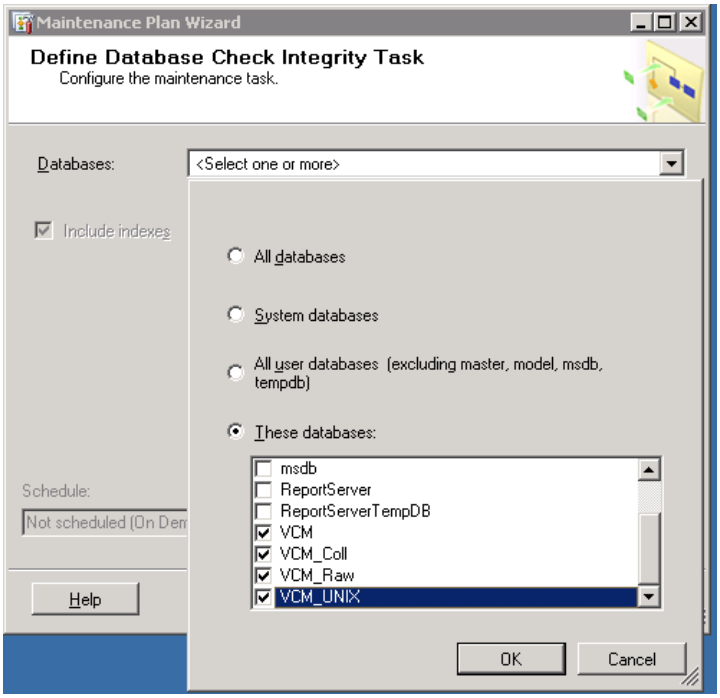
5. Set the scheduling properties for the job, as shown in this example. It is best to schedule the run time when the system is idle or has low usage.
6. After you have set the job schedule properties to your own specification, click **OK** to return to the Select Plan Properties page. Click **Next**. The Select Maintenance Tasks page appears.


Maintenance Plan Wizard
Select Maintenance Tasks
Which tasks should this plan perform?
Select one or more maintenance tasks:
Check Database Integrity
Shrink Database
Reorganize Index
Rebuild Index
Update Statistics
Clean Up History
Execute SQL Server Agent Job
Back Up Database (Full)
Back Up Database (Differential)
Back Up Database (Transaction Log)
Maintenance Cleanup Task
The History Cleanup task deletes historical data about Backup and Restore, SQL Server Agent, and Maintenance Plan operations. This wizard allows you to specify the type and age of the data to be deleted.
Help
< Back
Next >
Finish
Cancel

7. Select the maintenance tasks to be performed. Select **Check Database Integrity**, **Rebuild Index**, **Update Statistics**, and **Clean Up History**. Click **Next**. The Select Maintenance Task Order page appears.

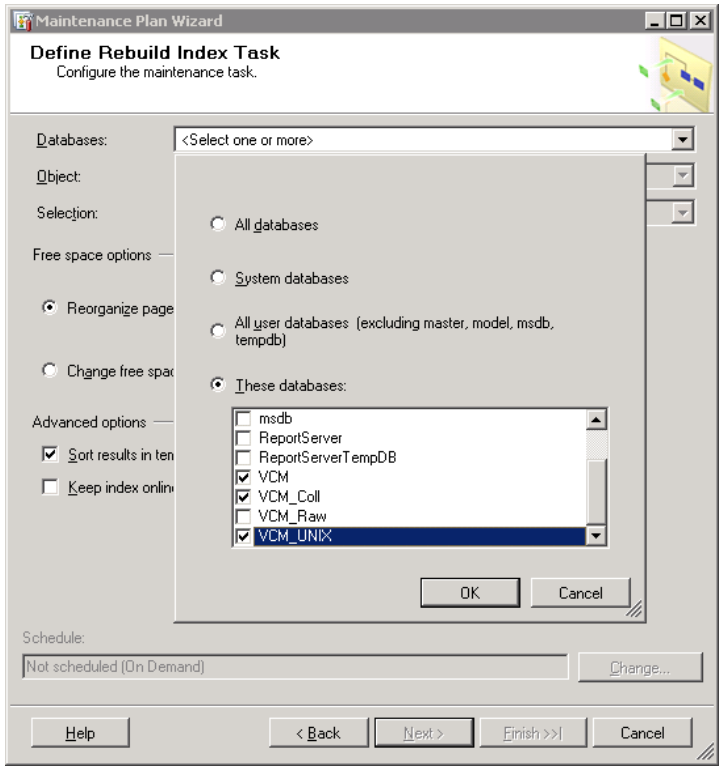

Maintenance Plan Wizard
Select Maintenance Task Order
In which order should these tasks be performed?
Select the order for the tasks to execute:
Check Database Integrity
Rebuild Index
Update Statistics
Clean Up History
Move Up...
Move Down...
The Check Database Integrity task performs internal consistency checks of the data and index pages within the database.
Help
< Back
Next >
Finish
Cancel

8. Specify the order for the maintenance tasks to be performed. Click **Next**. The Define Database Check Integrity Task page appears.



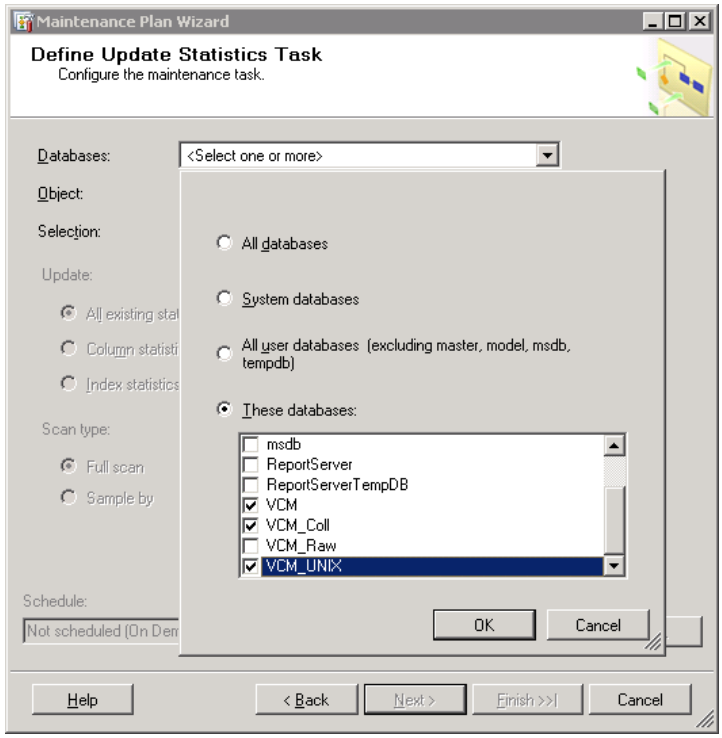
9. Click the Databases drop down menu. Select the CSI_Domain, VCM, VCM_Coll, VCM_Raw, and VCM_UNIX databases for the integrity check, and then click **OK**. When the databases are selected, Specific databases appears in the drop down field. Check the option **Include indexes**. Click **Next**. The Define Rebuild Index Task page appears.

NOTE Select the databases shown here, including the VCM_Raw database. The VCM_Raw database contains transient data, which is consumed by the other databases. For this reason, you should have the SQL Server 2005 Maintenance Plan check its integrity.

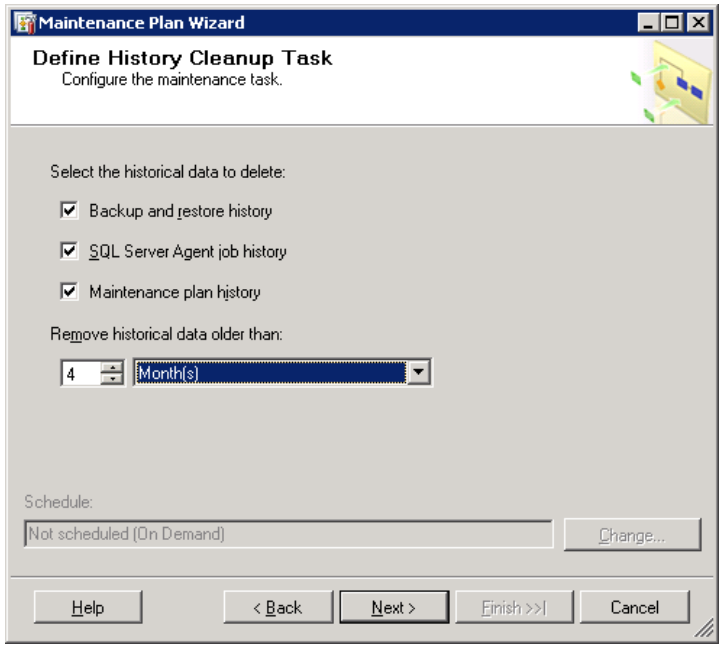


10. Specify how the Maintenance Plan should rebuild the Index. Click the Databases drop down menu. Select the CSI_Domain, VCM, VCM_Coll, and VCM_UNIX databases, and then click OK. When the databases are selected, Specific databases appears in the drop down field. In the **Advanced options** area of the dialog box, select **Sort results in tempdb**. Click **Next**. The Define Update Statistics Task page appears.

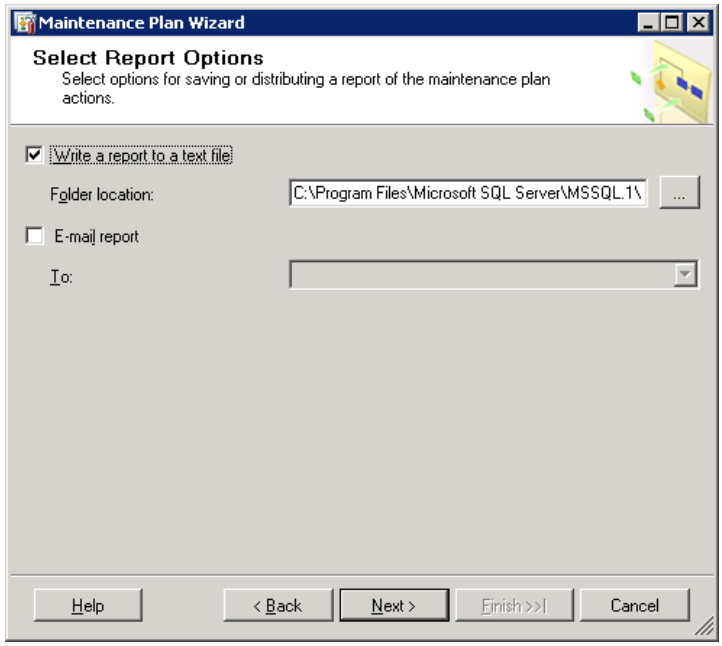
NOTE It is not necessary to rebuild the Index for the VCM_Raw database.



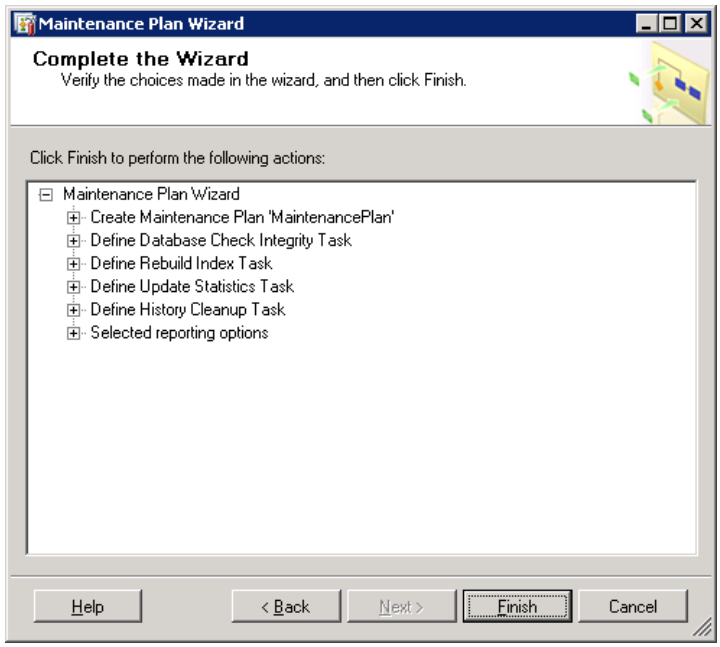
11. Specify how the Maintenance Plan should update the database statistics. Click the Databases drop down menu. Select the CSI_Domain, VCM, VCM_Coll, and VCM_UNIX databases, and then click **OK**. When the databases are selected, Specific databases appears in the drop down field. Click **Next**. The Define History Cleanup Task page appears.



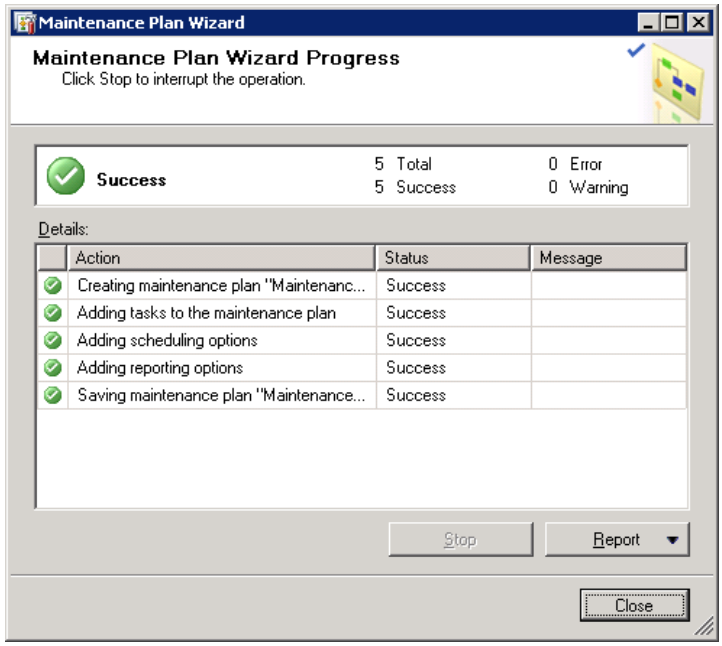
12. Specify the historical data to be removed from the SQL Server 2005 machine. VMware recommends saving historical data for four months, so set the option to 4 Months. The default setting is four weeks. Click **Next**. The Select Report Options page appears.



13. Select **Write a report to a text file**, and specify the folder location. Writing the report to a file saves a record of the maintenance plan actions for future reference. Click **Next**. The Complete the Wizard page appears.



14. Verify the selections in the Maintenance Plan Wizard. Expand the tree selections to view the settings. Click **Finish**. The Maintenance Plan Wizard Progress page appears.



15. When the Maintenance Plan Wizard completes, verify that the actions specified in the wizard were successful. To view, save, copy, or send the report, click **Report** and select an option.

You have now established a routine maintenance plan to assure that SQL Server 2005 continues to operate efficiently.

Incorporate the VCM CMDB into your Backup/Disaster Recovery Plans

Consider your VCM CMDB as you would any other SQL database in your environment. Take the necessary steps to have it incorporated into your corporate strategy for Backup/Disaster Recovery at this time.

Troubleshooting Problems with VCM

A

This chapter provides important information that will help you troubleshoot issues that may occur during the VCM software installation, upgrade, or use. This chapter describes resolving the following issues:

- Missing Patch Assessment Results
- Reports and Node Summaries Problems
- Protected Storage Errors
- Resetting the Require Secure Channel (SSL)
- Report Parameter Error

Evaluating Missing UNIX Patch Assessment Results

Before you can install patches, VCM Patching for UNIX patch assessments must complete successfully by displaying the assessment results. If a UNIX patch assessment does not return any results, the problem may be due to one of the following reasons.

- The assessment template may contain patch bulletins that do not match the selected machine type.
- The selected patch may not match the machine architecture; you must select 32-bit patches for 32-bit machines, and 64-bit patches for 64-bit machines.
- If you have defined a custom filter for Patch Assessment, it may not be including any of the bulletins that apply to the selected machine type. Certain filter attributes may not apply to bulletins across all platforms. For example, Severity is not used by some platforms. If you have defined a filter based on Severity, you would not include in your assessment any bulletins that do not have Severity set.
- The bulletins may not be in the required location on the Agent machine, which could occur for several reasons. Review the following list, and then check your UNIX Agent machine to confirm whether the bulletins exist in the correct location. Consider updating your UNIX Agents to 5.3.
    - The Agent version and UNIX platform support for Patch Assessment may not match.
        - Agent versions prior to 5.0 do not support UNIX Patch Assessment.
        - Support for Patch Assessment was added for some UNIX platforms in 5.0, but the patch assessment required manual distribution of bulletin information to the UNIX Agent machine to perform the assessment.
        - Support for additional UNIX platforms was added in 5.1, along with the automated distribution of bulletin information to Agent machines.
    - The process of distributing the bulletin information to UNIX Agent machines has failed.

- The bulletin information was removed from the UNIX Agent machine.
- Bulletin information may not be loaded on your Collector. If the Check for Updates action is indicating that no updates are available, then try the **Force** option on **Check for Updates**.
- An upgrade of the Collector to 5.3 failed to reprocess the bulletin information in order to extract the necessary information required for filtering. This step should have occurred automatically during the upgrade. Executing **Check for Updates** with the **Force** option may correct this problem.

- On older agents (VCM 5.1 and earlier) a **Machines - General** collection has not been done. Support for custom filters for UNIX Patch Assessment has been added to VCM, and can be used when assessing older agents. However, when assessing older agents (5.1 and earlier), you must have collected the **Machines - General** data class in order for the assessment to succeed. With the 5.1.x or later Agent, a **Machines - General** collection is not required.

Resolving Reports and Node Summaries Problems

After installing or upgrading VCM, problems with Visual Studio 2005 and the .NET Framework may occur. The following messages may appear:

- Server Unavailable
- The web application you are attempting to access on this web server is currently unavailable.
- Client found response content type of "text/html", but expected "text/xml".
- No results returned for specified parameters. (This error may occur even if the reports run and part of the report appears.)

To Resolve the Problem

If any of these messages occurs, follow the steps below to apply the hotfix.

1. Access the Microsoft Web site.
2. Search for the Knowledge Base article: KB913384. This article describes a hotfix for the following problem: A .NET Framework 2.0 application that runs under a user account context when no user profile is associated with the user account context may crash, or you may receive an access violation error message.
3. Download the hotfix that is applicable to your machine.
4. After you apply this hotfix, you must restart the machine.

Resolving Protected Storage Errors

When attempting to generate key pairs on the Agent Proxy machine, a protected storage error may occur. For example:

> CsiCommProxyUtil::wmain(): Failed to get protected storage for VCMv. HRESULT 0x8009000b = Key not valid for use in specified state.

If you encounter this type of error, use the workaround below to resolve the problem.

To Resolve the Problem

1. Open a command prompt.
2. Navigate to the `C:\Program Files\VMware\VCM\AgentData\protected` directory, and delete these two files: **`ECMv.csi.pds`** and **`ECMv.csi.pds.lck`**.
3. Execute the following command: **`GenerateAgentProxyKeys.cmd`**.
4. Verify that the following files were generated:

   ```
   <machine>_securecomm_public_key.txt
   ```

   ```
   <machine>_ssh_public_key.txt
   ```

5. From the command prompt, execute the following command: **`DatabaseUploadKey.cmd <machine>_securecomm_public_key.txt`** (where <machine> is the name of the Agent Proxy machine).

For more information about generating key pairs on the Agent Proxy Machine, see Chapter 6.

Resetting the Required Secure Channel (SSL)

When using SSL on the VCM collector, the following settings must be configured for VCM to work properly with SSL:

- Web.config file in the WebConsole directory
- Require secure channel (SSL) setting in IIS – for the VCM virtual directory
- IIS HTTP string http or https Database setting in VCM

When upgrading the Collector, the Require secure channel (SSL) check box in the VCM virtual directory properties may become unchecked. This problem can occur on a VCM Collector that is using SSL, when all of the settings listed above have been configured.

After upgrading VCM, log in and verify whether https is still required. If not, confirm that the settings to the Web.config configuration file, the VCM virtual directory, and the IIS settings are correct by using the procedures described in the sections below.

Updating the Web.config Configuration File

To modify the Web.config file, follow these steps:

1. On the Client/Collector machine where the SSL Certificate was issued, navigate to `C:\Program Files\VMware\VCM\WebConsole`.
2. Locate the `Web.config` file using Internet Explorer. Disable the **read-only** check box so that you can save the file by right-clicking the file, select **Properties**, and then uncheck the **read-only**check box. Click **OK**.
3. Open the `Web.config` file using Notepad.
4. In the `Web.config` file, search for the following tag:

   ```
   <add key="WebConsole.ReportingServices.ReportingService"
   value="https://COLLECTORNAME/ ReportServer/ReportService.asmx"
   ```

5. Verify that the URL listed after value begins with **https** instead of **http**.

Updating the VCM Virtual Directory

To update the VCM virtual directory, follow these steps:

1. Access Internet Information Services by opening a command prompt, and then typing `compmgmt.msc`.
2. Expand the **Services and Applications** node. Then expand **Internet Information Services | Web Sites | Default Web Site**.
3. Right-click the VCM virtual directory, and select **Properties**.
4. In the VCM Properties dialog box, click the **Directory Security** tab. In the **Secure Communications** panel, click **Edit**.
5. In the Secure Communications dialog box, check the **Require secure channel (SSL)** check box. Click **OK** twice to save the virtual directory properties.

Updating the IIS Settings in VCM

To modify the IIS settings in VCM, follow these steps:

1. Log into VCM, and then navigate to **Administration | Settings | General Settings | Database**.
2. In the Database settings, click to highlight the setting labeled **IIS HTTP string http or https**. Click **Edit Setting**, and then change the IIS HTTP string setting to **https**.

After performing these steps, you can operate VCM through a secure channel.

Resolving a Report Parameter Error

After upgrading VCM, if you encounter a problem with a report, your report may not have been uploaded correctly. This error can occur when reports have been overwritten, rather than removed in Report Manager. If the parameter values for the report have changed, the changes may not have been acknowledged by Report Manager when the report was uploaded and overwritten.

Before uploading the report again, you must first remove the existing version. To remove the existing report, follow the steps below. This procedure will create a new report instance in Report Manager.

1. Open Report Manager on the VCM Collector by entering http://collectorname/Reports.
2. Open the folder where the affected report resides. The VCM Reports. labeled ECM Reports, folders are as follows:
   - **ECMAD:** Active Directory
   - **ECMu:** UNIX
   - **RSCA:** RSCA
   - **Service Desk:** Service Desk and Change Reconciliation
   - **SMS:** SMS
   - **Standard:** Windows reports and Change Management and Compliance
   - **SUM:** VCM Patching
   - **Virtualization:** Virtualization

3. Click the **Show Details** button on the right hand of the screen.
4. Click the check box next to the affected report.
5. Click the **Delete** option. You will be prompted to be sure that you want to delete this item. Click **OK**.
6. Click **Upload File**.
7. On the **Upload File** screen, next to the **File to Upload** text box select **Browse**.
8. Select the report from the reports directory.
9. Click **OK**.

The report should now include all of the new parameter modifications.

Configuring a Collector as an Agent Proxy

B

Although it is not recommended, you can configure your Collector as an Agent Proxy. If you choose configuring your Collector as your Agent Proxy, the following configuration steps replace steps 1 - 4 in the "Configuring Agent Proxy Virtualization Collections" on page 118. You should perform the following configuration steps only if you are using your Collector machine as an Agent Proxy.

1. Verify membership to CSI_COMM_Proxy_SVC.
2. Generate key pairs.
3. Upload keys to database.

Verifying Membership to CSI_COMM_PROXY_SVC on the Agent Proxy Machine

Perform the following procedure on the Collector machine that you will be using as the Agent Proxy.

1. Click **Start | Administrative Tools | Computer Management**.
2. Expand the **Local Users and Groups** node, and then click **Groups**.
3. Double-click the **CSI_COMM_PROXY_SVC** group.
4. Add the Network Authority account to the CSI_COMM_PROXY_SVC group. This account is the VCM Collector Service account that was specified during installation.

   NOTE This is the Network Authority Account name and VCM Service (such as SAS) that you used during installation. For more information on the Network Authority Account, see About Available Accounts in the online Help.

5. Add any additional users that should have access to the Collector (as Agent Proxy), and then click **OK**.
6. If you made changes to the group membership, you MUST reboot the Collector machine to apply the changes.

NOTE If you need to replace a local user in the CSI_COMM_Proxy_SVC group with a new local user, the new account must have full control of `[drive]:\Program Files\VMware\VCM` and have full control of the Configuresoft registry key (`HKEY_LOCAL-MACHINE\Software\Configuresoft`).

If keys have already been generated, the `agentdata\protected` folder must be deleted and new keys

generated/uploaded and distributed.

To change the password for the new user account, you must log in as the user rather than allowing an administrator to reset the password. If the password is changed by the new user, the keys do not need to be regenerated.

Generating Key Pairs on the Agent Proxy Machine

Use the following procedure to log in to the Collector you are using as the Agent Proxy and generate the key pairs necessary for communication between an ESX/vSphere Server and the Agent Proxy. This procedure assumes that you are using default installation location the for Agent (`C:\WINDOWS\CMAgent`).

1. Open a Command Prompt on the Agent Proxy machine.
2. Change directory to: `[drive:]Program Files\VMware\VCM\Tools\Virtualization`.
3. At the command prompt, run the following command: `GenerateAgentProxyKeys`

NOTE If you receive an Access is denied error message, then one of the following problems has occurred: 1) You did not add users or groups to the CSI_COMM_PROXY_SVC group OR you did not reboot, or 2) You are not running in a CMD shell as a user in the CSI_COMM_PROXY_SVC group.

4. Verify that the following files were generated:

```
<machine>_securecomm_public_key.txt
<machine>_ssh_public_key.txt
```

NOTE Verify `<machine>` is the name of the Collector machine.

Uploading Keys to the Database

1. Login to the Collector machine and open a Command Prompt.
2. From the command prompt, change directory to:

```
<install_drive:>\Program Files\VMware\VCM\Tools\Virtualization
```

3. From the command prompt, execute the following command (where <machine> is the name of the Agent Proxy machine):

```
DatabaseUploadKey.cmd <machine>_securecomm_public_key.txt
```

After performing the above steps, go to "Configuring Agent Proxy Virtualization Collections" on page 118 workflow. Continue with "Configuring ESX/vSphere Servers" on page 123 and continue through the rest of the workflow.

Index

%

%Systemroot% environment variable **63**

A

about this book **9**
access by user **47**
accessing
compliance content 239
account
application services 14
collector services 14
network authority 13
Oracle collection user 110
active directory
(AD) 209
agent 213
collection results 223
configuration 216
data collection 220
domain controllers 209
getting started 209
network authority account 211
reference information 226
run determine forest action 218
run setup DCs action 218
AD (active directory) **209**
adding
assets hardware configuration 200
assets software configuration 202
ESX/vSphere servers 125
Mac OS X 94
Oracle Instances 109
repository sources 188
UNIX machines hosting Oracle 109
UNIX/Linux machines 81
Web Services user 129
administration
rights 13
ADProductInstall.exe for Windows **63**
agent
active directory 213
ADProductInstall.exe for Windows AD 63
binaries per OS 84, 97
CMAgentInstall.exe for Windows 63
installation 16, 61
installation, manually 62
installation, Oracle 109
installing
agent proxy 121
Mac OS X 97
platforms supported 40, 83
proxy
platform not supported 43
upgrading 43
upgrading manually 43
uninstall, Mac OS X 102
uninstall, UNIX/Linux 89
uninstalling 64
UNIX upgrade 40-41
upgrading 38
upgrading for UNIX 40
agent proxy
configuring 120
collecting machines data class 121
installing agent 121
installing agent proxy 122
licensing 120
configuring collector 265
installing 122
SSH key 122
agents
certificates 16
AgentUpgradeLocal.sh for UNIX **41**
application services
account 14
assets
configuration items 195
getting started 195
hardware configuration items 200
software configuration items 202
auditing **116**
authentication
server 15
automatic upgrade
Remote client 39

B

backup/disaster recovery plan **258**
binary mode, use for ftp **84, 97**
broadband **147**

C

certificates
agents 16
collector 15
enterprise 15
Enterprise Certificate 63
installing ESX Web Services 130
PKI 63
secure communication 15
Web Services
agent proxy 130

change detection
WCI 74
check
for UNIX/Linux updates 169
for Windows updates 159
CMAgentInstall.exe
for Windows 63
uninstalling agent 64
collect
package managers 187
repositories 187
collection results
AD 223
Oracle 114
Remote 157
SMS 229
UNIX/Linux 91
virtualization 135
WSUS 237
collection scripts
custom for WCI 77
collection user account
creating, Config User Action 110
creating, remote command 111
Oracle 110
collections
active directory 220
AD 216
exploring, Windows 68
Mac OS X 103
Oracle 114
patching 160
Remote 157
results, Mac OS X 106
SMS Client 229
SMS Server 228
troubleshooting vCenter Server 142
UNIX/Linux 90
vCenter Server data 137, 141-142
virtualization 134
WCI 73
Windows machines 67
WSUS, client 236
WSUS, server 236
collector
aware of Remote client 156
certificates 15
importing content 239
install before agents 83, 97
lock request 63
collector services
account 14
compliance
checking Windows 71
checking, UNIX/Linux 91
content, accessing 239
imported content 239
Mac OS X 106
rule
remediation
software provisioning 191
software provisioning 190
components
getting started 47
configurations
AD 216
assets 195
collector as agent proxy 265
database file growth 249
installation 12
modifying hardware, assets 196
modifying software, assets 198
updating Web.config 261
Web Services for ESX/vSphere 128
configuring
popup blocker 48
vSphere Client Plug-in 144
content for compliance **239**
importing to collector 239
location 239
wizard 243
copying
files to ESX/vSphere servers 124
creating
Oracle collection user account 110-111
csi.config file **85, 88, 98, 101**
CSI_AGENT_RUN_OPTION **88**
CSI_COMM_Proxy_SVC
agent proxy 122
csiprep.config
ESX servers 124
csiprep.py **125**
ESX servers 124
custom filter sets
for Remote 156
customization
component settings 247
for your environment 115

D

database
backup/disaster recovery plan 258
recovery settings 250
deploying
AD agent 213
AD to domain controllers 216
patches, UNIX/Linux 175
patches, Windows machines 165
deployment tool
virtualization 120
determine forest action
running for AD 218
developing
custom collection scripts 77
dialup **147**

disabling
UAC on Windows machines 61, 65, 214
disaster recovery plan 258
discovering
domain controllers, AD 211
Oracle Instances 109
Windows machines 53, 56
domain controllers
active directory 209
deploying AD 216
domains
active directory 209
AD, confirming presence 210
verifying 53

E

enabling
popup blocker 48
enterprise
certificates 15
environment variable, %Systemroot% 63
ESX 2.5 only
setting up VirtualCenter 134
ESX certificate
Web services
agent proxy 130
ESX servers
configuring 123
adding 125
licensing 126
csiprep.config 124
csiprep.py 124-125
SSH key 124
virtualization 123
ESXi 118
exploring
AD collection results 223
assessment results, UNIX 173
assessment results, Windows 165
collection results
Oracle 114
UNIX/Linux 91
virtualization 135
Windows 68
imported content 239
Remote collection results 157

F

filter sets
imported content 239
in Remote settings 156
Remote 156
forest
run determine forest action 218
forests
active directory 209
foundation checker 241
installation 242
ftp, use binary mode 84, 97

G

getting started 53
active directory 209
assets 195
auditing 116
components, tools 47
deploy patches, UNIX/Linux 175
deploy patches, Windows 165
explore assessment results, UNIX 173
explore assessment results, Windows 165
launch assessment 161
launching 48
logging on 48
patching collection 160
Remote 147
SMS 227
tools 241
virtualization 117
vSphere Client Plug-in 145
WCI 72
WCI PowerShell scripts 75
WSUS 235
Getting Started
Using Patching 159

H

HTTP agent, port number 63

I

IIS settings
updating 262
import/export wizard 243
importing content
content wizard 239
information bar in portal 49
install
Windows machines 53
installation
agent 16
agent on Mac OS X machines 97
agent on Red Hat, SUSE 83
agent on UNIX/Linux machines 83
agent on Windows machines 61
agent, manually 62
agent, UNIX 83, 97
check prerequisites 13
configurations 12
ESX Web Services certificate 130
foundation checker 242
maintenance after 247
navigating process of 19
preparing 11
prerequisites 13
Remote client 149
command line 151
remote command 152

tools 13, 241
understanding configurations 12
using installation manager 12
InstallCMAgent 87, 100
installing
Package Manager for Windows 184
Package Studio 182
packages 189
repositories 181
integration
Service Desk 205

J

job manager 241-242
job status reporting
WCI 74
jobs history
provisioning 190

L

LAN 147
launch an assessment 161
launching
content wizard 239
license
Windows machines 53
licensing
AD agent 213
agent proxy 120
ESX servers 126
virtual machine hosts 127
ESX/vSphere servers 126-127
Mac OS X 96
UNIX/Linux machines 82
Windows machines 59
local package
UNIX agent upgrade 40
location for compliance content 239
lock request, submit from collector 63

M

Mac OS X
adding 94
agent
installing 97
agent, uninstall 102
collection 103
collection results 106
licensing 96
maintenance
after installation 247
backup/disaster recovery plan 258
configure database file growth 249
create plan 250
customize settings 247
database recovery settings 250
modifying
assets hardware configurations 196
assets software configurations 198

N

network authority account 13
AD 211
checking 54
node summaries
resolving problems 260

O

operating systems
agent binaries 84, 97
Oracle
10g installations 113
Add/Edit Instance 109
adding instances 109
agent installation 109
collection results 114
collection user account 110, 113
collections 114
Config User Action 110
discovering instances 109
permissions 113
reference information 114
remote command 111
Oracle Database
Removing access 112
overview
vSphere Client Plug-in 143

P

Package Manager for Windows
installing 184
package managers
collect 187
Package Studio
installing 182
packages
importing content 239
installing 189
patching
check for updates, UNIX/Linux 169
check for updates, Windows 159
collection 160
UNIX assessment results troubleshooting 259
permissions
Oracle 113
planning maintenance 250
platforms
agent proxy support 43
UNIX agent support 40, 83
popup blocker
configure or enable 48
port number for HTTP agent install 63
port number for UNIX agent install 89, 102
portal
familiarizing 48
information bar 49
sliders 50
toolbar 49

PowerShell
executing for WCI 76
for Windows Custom Info 72
scripts, troubleshooting 80
signing scripts for WCI 76
WCI getting started 75
prerequisites
check for installation 13
for upgrading 35
vCenter Server collections 137
protected storage
resolving problems 260
provisioning
compliance
remediation 191
compliance rule 190
install agent 16
jobs History 190
Public Key Infrastructure (PKI) **63**
purge
for WCI 74

R

recovery plan **258**
Red Hat
install UNIX agent 83
Red Hat workstations
upgrading 40, 82
reference information
AD 226
assets 203
customizing your environment 146
Oracle 114
Service Desk 207
SMS 233
WSUS 238
registering
vSphere Client Plug-in 45, 143, 146
remediation
compliance rule
software provisioning 191
Remote
collection results 157
collections 157
filter sets 156
getting started 147
settings 156
filter sets 156
virtual directory 14
Remote client
automatic upgrade 39
collector aware 156
installing 149
command line 151
remote command 152
remote package
UNIX agent upgrade 41
repairing
uninstall, troubleshooting 34
reports
parameter error, resolving 262
resolving problems 260
WCI 75
repositories
collect 187
installing 181
repository sources
adding 188
resetting
required secure channel (SSL) 261
resolving reports parameter error **262**
results
collection, Mac OS X 106
collection, SMS 229
collection, WSUS 237
imported content 239
virtualization 135
rights
administration 13
running
determine forest action for AD 218
setup DCs action for AD 218

S

scripts
PowerShell 75
running on ESX/vSphere server 124
secure communication **15**
server
authentication 15
Service Desk integration **205**
settings
cusomizing for components 247
database recovery 250
remote 156
VM hosts 134
setup DCs action
running for AD 218
signing
PowerShell scripts 76
sliders
in portal 50
SMS
client collections 229
collection results 229
getting started 227
server collections 228
sources
repository sources
adding 188
SQL*Plus
Oracle 113
SSH key
agent proxy 122
ESX servers 124

SSL
resetting required secure channel 261
SUSE
install UNIX agent 83

T

templates
for compliance 239
ToCMBase64String **77**
toolbar
in portal 49
tools
foundation checker 241
getting started 47, 241
import/export, content 241
installation 13, 241
job manager 241-242
troubleshooting **259**
PowerShell scripts 80
vCenter Server data collections 142

U

UAC
disabling on Windows machines 61, 65, 214
uninstall
agent 64
agent, Mac OS X 102
agent, UNIX/Linux 89
troubleshooting 34
UNIX agent
platform support 40, 83
port number 89, 102
upgrading 40
local package 40
remote package 41
UNIX/Linux
agent uninstall 89
AgentUpgradeLocal.sh 41
assessments results, troubleshooting 259
check for updates 169
collections 90
machines, adding 81
machines, licensing 82
updates
check for content wizard 245
check for UNIX/Linux 169
check for Windows 159
updating
IIS settings 262
virtual directory 262
Web.config file 261
upgrading **35**
agent 38
agent proxy 43
agent proxy manually 43
automatic 39
failed, troubleshooting 34
Red Hat workstations 40, 82
UNIX agent 40
local package 40
remote package 41
virtualization 42
vSphere Client Plug-in 45, 146
user access **47**

V

vCenter Server **118**
data collections 137, 141
verifying
domain controllers, AD 213
domains 53
virtual center
collecting 134
virtual directory
Remote 14
updating 262
virtual machine hosts
licensing
ESX servers 127
virtualization
collecting 134
results 135
collections 134
configuration
workflow 119
configuring
agent proxy 120
ESX servers 123
web services 128
deployment tool 120
ESX servers 123
getting started 117
upgrading 42
web services
user roles 129
VM hosts
settings 134
vSphere Client Plug-in
configuring 144
getting started 145
overview 143
registering 143
upgrading 45, 146

W

WCI
change detection 74
collection 73
custom collection scripts 77
executing PowerShell scripts 76
getting started 72
job status reporting 74
purge 74
running reports 75

Web Services
configuring
ESX certificate 130
settings 134
virtualization 128
settings 134
user roles
virtualization 129
user, adding 129
Web.config file 261
Windows
check for updates 159
Windows Custom Information (WCI) 72
Windows machines
collecting 67
disabling UAC 61, 65, 214
discover, license, install 53
discovering 56
install agent 61
licensing 59
uninstalling agent 64
Windows Server Update Services (WSUS) 235
wizards
content 243
import/export 243
workstations
upgrading Red Hat 40, 82
WSUS
collection results 237
collections, client 236
collections, server 236
getting started 235